

June 2011

DEPARTMENT OF DEFENSE

Further Actions Needed to Institutionalize Key Business System Modernization Management Controls



G A O

Accountability * Integrity * Reliability

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUN 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE Department of Defense: Further Actions Needed to Institutionalize Key Business System Modernization Management Controls				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Government Accountability Office, 441 G Street NW, Washington, DC, 20548				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 75	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Why GAO Did This Study

For decades, the Department of Defense (DOD) has been challenged in modernizing its timeworn business systems. Since 1995, GAO has designated DOD's business systems modernization program as high risk. Between 2001 and 2005, GAO reported that the modernization program had spent hundreds of millions of dollars on an enterprise architecture and investment management structures that had limited value. Accordingly, GAO made explicit architecture and investment management-related recommendations. Congress included provisions in the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 that were consistent with GAO's recommendations and required GAO to assess DOD's actions to comply with these provisions. To do so, GAO reviewed documents and interviewed military officials on the progress the military departments have made relative to developing their respective parts of the federated business enterprise architecture and establishing investment management structures and processes.

What GAO Recommends

Because GAO has existing recommendations that address the long-standing challenges discussed in this report, it is making no further recommendations in these areas. GAO is recommending that DOD complete the implementation of the reorganization of key organizations. DOD agreed with GAO's recommendation.

DEPARTMENT OF DEFENSE

Further Actions Needed to Institutionalize Key Business System Modernization Management Controls

What GAO Found

DOD continues to take steps to comply with the act's provisions and to satisfy relevant system modernization management guidance. Collectively, these steps address several statutory provisions and best practices concerning the business enterprise architecture, budgetary disclosure, and review of systems costing in excess of \$1 million. However, long-standing challenges that GAO previously identified remain to be addressed in order for DOD to be in compliance with guidance and the act. In particular,

- While DOD continues to release updates to its enterprise architecture, the architecture has yet to be augmented by a coherent family of component architectures. In this regard, each of the military departments has made progress in managing its respective enterprise architecture program since GAO last reported in 2008. However, each has yet to address key elements, including developing the architecture content, to advance to a level that could be considered mature. For example, while each department has established or is in the process of establishing an executive committee with responsibility and accountability for the enterprise architecture, none has fully developed an enterprise architecture methodology or a well-defined business enterprise architecture and transition plan to guide and constrain business transformation initiatives.
- DOD continues to establish investment management processes, but neither DOD-level organizations nor the military departments have defined the full range of project-level and portfolio-based IT investment management policies and procedures that are necessary to meet the investment selection and control provisions of the Clinger-Cohen Act of 1996. Specifically, with regard to project-level practices, DOD enterprise, Air Force, and Navy have yet to fully define 56 percent of the practices, and Army has yet to do so for 78 percent of the practices. With regard to the portfolio-level practices, DOD enterprise, Air Force, and Navy have yet to fully define 80 percent and Army has yet to do so for any of the practices. In addition, while DOD largely followed its certification and oversight processes, key steps were not performed. For example, as part of the certification process, DOD performed three process assessments specified in DOD guidance, such as assessing investment alignment with the architecture, but did not validate the results of the assessment, thus increasing the risk that certification decisionmaking was based on inaccurate and unreliable information.

It is essential that DOD address GAO's existing recommendations aimed at addressing these long-standing challenges, as doing so is critical to the department's ability to establish the full range of institutional management controls needed to address its business systems modernization high-risk program. Department officials attributed the state of progress in part to the uncertainty and pending decisions surrounding the roles and responsibilities of key organizations and senior leadership positions as well as the lack of resources (i.e., people and funding).

Contents

Letter		1
	Background	3
	DOD Continues to Strengthen Management of Its Business Systems Modernization, but Long-standing Challenges Remain	27
	Conclusions	60
	Recommendation for Executive Action	61
	Agency Comments and Our Evaluation	61

Appendix I	Objective, Scope, and Methodology	64
-------------------	--	-----------

Appendix II	Comments from the Department of Defense	68
--------------------	--	-----------

Appendix III	GAO Contact and Staff Acknowledgments	70
---------------------	--	-----------

Tables		
	Table 1: Stage 2 Critical Processes and Associated Key Practices	14
	Table 2: Stage 3 Critical Processes and Associated Key Practices	15
	Table 3: DOD Business Systems Modernization Governance Entities' Roles, Responsibilities, and Composition	17
	Table 4: DOD Investment Tiers	20
	Table 5: Description of Progress for Enterprise Architecture Core Elements Previously Reported as Not Fully Satisfied by One or More Military Departments	30
	Table 6: Summary of Key Practices for Stage 2 Critical Processes– Building the Investment Foundation	46
	Table 7: Summary of Key Practices for Stage 3 Critical Processes– Developing a Complete Investment Portfolio	48

Figures		
	Figure 1: Simplified View of DOD Organizational Structure	4
	Figure 2: The Five ITIM Stages of Maturity with Critical Processes	13

Abbreviations

ASD(NII)/DOD CIO	Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer
BEA	business enterprise architecture
CIO	chief information officer
DITPR	Defense Information Technology Portfolio Repository
DOD	Department of Defense
IRB	investment review board
IT	information technology
ITIM	Information Technology Investment Management
IV&V	independent verification and validation
NDAA	National Defense Authorization Act
OMB	Office of Management and Budget
PMRT	Project Management Resource Tool
SNAP-IT	Select and Native Programming Data Input System—Information Technology

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

June 29, 2011

Congressional Committees

For decades, the Department of Defense (DOD) has been challenged in modernizing its timeworn business systems.¹ In 1995, we designated the department's business systems modernization program as high risk, and we continue to designate it as such today.² As our research on public and private sector organizations has shown, two essential ingredients to a successful systems modernization program are an effective institutional approach to managing information technology (IT) investments and a well-defined enterprise architecture.³ For its business systems modernization, DOD is developing and using a federated business enterprise architecture, which is a coherent family of parent and subsidiary architectures, to help modernize its nonintegrated and duplicative business operations and the systems that support them.

In May 2001,⁴ we recommended that the Secretary of Defense establish the means for effectively developing an enterprise architecture and a corporate, architecture-centric approach to investment control and decision making. Yet, between 2001 and 2005, we reported that the department's business systems modernization program continued to lack both of these approaches, concluding in 2005 that hundreds of millions of dollars had been spent on a business enterprise architecture and

¹Business systems support DOD's business operations, such as civilian personnel, finance, health, logistics, military personnel, procurement, and transportation.

²GAO, *High-Risk Series: An Update*, [GAO-11-278](#) (Washington, D.C.: February 2011).

³An enterprise architecture, or modernization blueprint, provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., federal department or agency) or a functional or mission area that cuts across more than one organization (e.g., financial management). This picture consists of snapshots of the enterprise's current or "as is" operational and technological environment and its target or "to be" environment, and contains a capital investment road map for transitioning from the current to the target environment. These snapshots consist of "views," which are basically one or more architecture products that provide conceptual or logical representations of the enterprise.

⁴GAO, *Information Technology: Architecture Needed to Guide Modernization of DOD's Financial Operations*, [GAO-01-525](#) (Washington, D.C.: May 17, 2001).

investment management structures that had limited value.⁵ Accordingly, we made additional, explicit architecture and investment management-related recommendations to address these continuing deficiencies.

To further assist DOD in addressing these modernization management challenges, Congress included provisions in the Ronald W. Reagan National Defense Authorization Act (NDAA) for Fiscal Year 2005⁶ that were consistent with our recommendations. More specifically, section 332 of the act required the department to, among other things, (1) develop a business enterprise architecture and a transition plan for implementing the architecture, (2) identify systems information in its annual budget submission, (3) establish a system investment approval and accountability structure along with an investment review process, and (4) certify and approve any system modernizations costing in excess of \$1 million. The act⁷ further required that the Secretary of Defense submit an annual report to congressional defense committees on DOD's compliance with certain requirements of the act not later than March 15 of each year, from 2005 through 2013. Additionally, the act directed us to submit to these congressional committees—within 60 days of DOD's report submission—an assessment of the department's actions to comply with these requirements.

Accordingly, as agreed with your office, the objective of our review was to assess the actions by DOD to comply with the above four provisions of section 332 of the act. To address the provisions of the act related to

⁵GAO, *DOD Business Systems Modernization: Long-standing Weaknesses in Enterprise Architecture Development Need to Be Addressed*, [GAO-05-702](#) (Washington, D.C.: July 22, 2005); *DOD Business Systems Modernization: Billions Being Invested without Adequate Oversight*, [GAO-05-381](#) (Washington, D.C.: Apr. 29, 2005); *DOD Business Systems Modernization: Limited Progress in Development of Business Enterprise Architecture and Oversight of Information Technology Investments*, [GAO-04-731R](#) (Washington, D.C.: May 17, 2004); *DOD Business Systems Modernization: Important Progress Made to Develop Business Enterprise Architecture, but Much Work Remains*, [GAO-03-1018](#) (Washington, D.C.: Sept. 19, 2003); *Business Systems Modernization: Summary of GAO's Assessment of the Department of Defense's Initial Business Enterprise Architecture*, [GAO-03-877R](#) (Washington, D.C.: July 7, 2003); *Information Technology: Observations on Department of Defense's Draft Enterprise Architecture*, [GAO-03-571R](#) (Washington, D.C.: Mar. 28, 2003); *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, [GAO-03-458](#) (Washington, D.C.: Feb. 28, 2003); and [GAO-01-525](#).

⁶Pub. L. No. 108-375, § 332, 118 Stat. 1811, 1851-1856 (Oct. 28, 2004) (codified in part at 10 U.S.C. § 2222).

⁷10 U.S.C. § 2222(i), as amended.

enterprise architecture and investment management, we focused on the progress the military departments have made relative to developing their respective parts of the federated business enterprise architecture and establishing investment management structures and processes as required by statute, using the results of our prior reports as a baseline.⁸ To address the budgetary disclosure and certification provisions of the act, we reviewed the department's report to Congress, which was submitted on May 4, 2011, and evaluated the information used to satisfy the budget submission and investment review, certification, and approval aspects of the act.

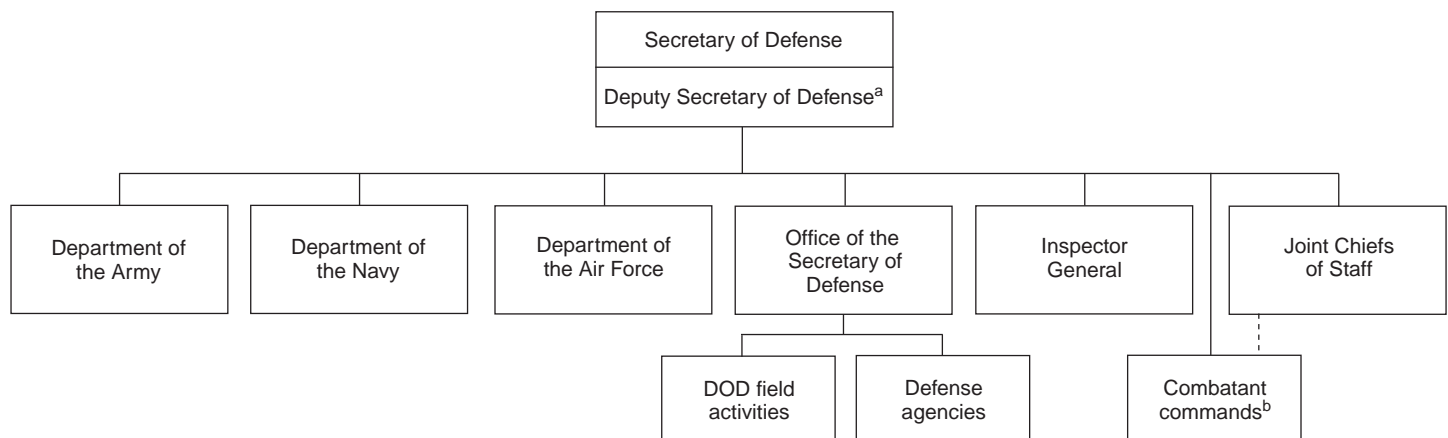
We conducted this performance audit at DOD and military department offices in Arlington, Virginia, from January to June 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Details on our objective, scope, and methodology are contained in appendix I.

Background

DOD is a massive and complex organization entrusted with more taxpayer dollars than any other federal department or agency. Organizationally, the department includes the Office of the Secretary of Defense, the Joint Chiefs of Staff, the military departments, numerous defense agencies and field activities, and various unified combatant commands that are responsible for either specific geographic regions or specific functions. (See fig. 1 for a simplified depiction of DOD's organizational structure.)

⁸GAO, *DOD Business Systems Modernization: Recent Slowdown in Institutionalizing Key Management Controls Needs to Be Addressed*, [GAO-09-586](#) (Washington, D.C.: May 18, 2009); *DOD Business Systems Modernization: Military Departments Need to Strengthen Management of Enterprise Architecture Programs*, [GAO-08-519](#) (Washington D.C.: May 12, 2008); *Business Systems Modernization: Department of the Navy Needs to Establish Management Structure and Fully Define Policies and Procedures for Institutionally Managing Investments*, [GAO-08-53](#) (Washington, D.C.: Oct. 31, 2007); *Business Systems Modernization: Air Force Needs to Fully Define Policies and Procedures for Institutionally Managing Investments*, [GAO-08-52](#) (Washington, D.C.: Oct. 31, 2007).

Figure 1: Simplified View of DOD Organizational Structure



Source: GAO based on DOD documentation.

^aThe Deputy Secretary of Defense serves as the Chief Management Officer, who provides focused and sustained leadership over DOD's business transformation efforts.

^bThe Chairman of the Joint Chiefs of Staff serves as the spokesperson for the commanders of the combatant commands, especially on the administrative requirements of the commands.

In support of its military operations, DOD performs an assortment of interrelated and interdependent business functions, such as logistics management, procurement, health care management, and financial management. As we have previously reported,⁹ the DOD systems environment that supports these business functions is overly complex and error prone, and is characterized by (1) little standardization across the department, (2) multiple systems performing the same tasks, (3) the same data stored in multiple systems, and (4) the need for data to be entered manually into multiple systems. The department recently requested about \$17.3 billion for its business systems environment and IT infrastructure investments for fiscal year 2012. According to the department's systems inventory, this environment is composed of 2,258 business systems and includes 335 financial management, 709 human resource management, 645 logistics, 243 real property and installation, and 281 weapon acquisition management systems.

⁹GAO, *Business Systems Modernization: DOD Continues to Improve Institutional Approach, but Further Steps Needed*, [GAO-06-658](#) (Washington, D.C.: May 15, 2006).

DOD currently bears responsibility, in whole or in part, for 14 of the 30 programs across the federal government that we have designated as high risk because they are highly susceptible to fraud, waste, abuse, and mismanagement.¹⁰ Seven of these areas are specific to the department,¹¹ and seven other high-risk areas are shared with other federal agencies.¹² Collectively, these high-risk areas relate to DOD's major business operations that are inextricably linked to the department's ability to perform its overall mission and directly affect the readiness and capabilities of U.S. military forces and can affect the success of a mission. In particular, the department's nonintegrated and duplicative systems impair its ability to combat fraud, waste, and abuse.¹³ As such, DOD's business systems modernization is one of the high-risk areas and is an essential enabler in addressing many of the department's other high-risk areas. For example, modernized business systems are integral to the department's efforts to address its financial, supply chain, and information security management high-risk areas.

¹⁰GAO, *High-Risk Series: An Update*, [GAO-11-278](#) (Washington, D.C.: February 2011).

¹¹These seven high-risk areas include DOD's overall approach to business transformation, business systems modernization, contract management, financial management, supply chain management, support infrastructure management, and weapon systems acquisition.

¹²The seven governmentwide high-risk areas include disability programs, ensuring the effective protection of technologies critical to U.S. national security interests, interagency contracting, information systems and critical infrastructure, information sharing for homeland security, human capital, and real property.

¹³GAO, *DOD Business Systems Modernization: Planned Investment in Navy Program to Create Cashless Shipboard Environment Needs to Be Justified and Better Managed*, [GAO-08-922](#) (Washington, D.C.: Sept. 8, 2008); *DOD Travel Cards: Control Weaknesses Resulted in Millions of Dollars of Improper Payments*, [GAO-04-576](#) (Washington, D.C.: June 9, 2004); *Military Pay: Army National Guard Personnel Mobilized to Active Duty Experienced Significant Pay Problems*, [GAO-04-89](#) (Washington, D.C.: Nov. 13, 2003); and *Defense Inventory: Opportunities Exist to Improve Spare Parts Support Aboard Deployed Navy Ships*, [GAO-03-887](#) (Washington, D.C.: Aug. 29, 2003).

Enterprise Architecture and IT Investment Management Controls Are Critical to Achieving Successful Systems Modernization

Effective use of a well-defined enterprise architecture is a hallmark of successful organizations and a basic tenet of organizational transformation and systems modernization. Since the early 1990s, we have promoted federal department and agency enterprise architecture adoption as an essential means to achieving a desired end: having operational and technology environments that maximize institutional mission performance and outcomes.¹⁴ Congress, the Office of Management and Budget (OMB), and the federal Chief Information Officers (CIO) Council have also recognized the importance of an architecture-centric approach to modernization. The Clinger-Cohen Act of 1996, among other things, requires the CIOs of federal departments and agencies to develop, maintain, and facilitate architectures as a means of integrating business processes and agency goals with IT.¹⁵ Further, the E-Government Act of 2002 established the OMB Office of Electronic Government and assigned it, among other things, responsibility for overseeing the development of enterprise architectures within and across agencies.¹⁶ In addition, OMB, the CIO Council, and we have issued guidance that emphasizes the need for system investments to be consistent with these architectures.¹⁷ For example, in April 2003 and in August 2010, we published a framework¹⁸ that emphasizes the importance of having an enterprise architecture as a critical frame of reference for organizations when they are making IT investment decisions. Also, in December 2008, OMB issued guidance¹⁹ that addresses system investment compliance with agency architectures.

¹⁴GAO, *Strategic Information Planning: Framework for Designing and Developing System Architectures*, [GAO/IMTEC-92-51](#) (Washington, D.C.: June 1992).

¹⁵40 U.S.C. § 11315(b)(2).

¹⁶44 U.S.C. § 3602(f)(14).

¹⁷GAO, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)*, [GAO-10-846G](#) (Washington, D.C.: August 2010); *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C.: March 2004); *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management, Version 1.1*, [GAO-03-584G](#) (Washington, D.C.: April 2003); *OMB Capital Programming Guide, Version 1.0* (July 1997); and CIO Council, *A Practical Guide to Federal Enterprise Architecture, Version 1.0* (February 2001).

¹⁸[GAO-10-846G](#) and [GAO-03-584G](#).

¹⁹OMB, *Improving Agency Performance Using Information and Information Technology (Enterprise Architecture Assessment Framework v 3.0)* (December 2008).

A corporate approach to IT investment management is another important characteristic of successful public and private organizations. Recognizing this, the Clinger-Cohen Act²⁰ requires OMB to establish processes to analyze, track, and evaluate the risks and results of major capital investments in IT systems made by executive agencies.²¹ In response to the Clinger-Cohen Act and other statutes, OMB developed policy and issued guidance for planning, budgeting, acquisition, and management of federal capital assets.²² We have also issued guidance in this area that defines institutional structures (such as investment boards), processes for developing information on investments (such as cost/benefit), and practices to inform management decisions (such as whether a given investment is aligned with an enterprise architecture).²³

Enterprise Architecture: A Brief Description

An enterprise architecture provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., a federal department or agency) or a functional or mission area that cuts across more than one organization (e.g., financial management). An architecture describes the enterprise in logical terms (such as interrelated business processes and business rules, information needs and flows, and work locations and users) as well as in technical terms (such as hardware, software, data, communications, security attributes, and performance standards). It provides these perspectives both for the enterprise's current environment and for its target environment, and it provides a transition plan for moving from the current to the target environment. This transition plan provides a temporal road map for moving between the two environments and

²⁰ 40 U.S.C. § 11302(c)(1). The Clinger-Cohen Act expanded the responsibilities of OMB and the agencies that had been established under the Paperwork Reduction Act of 1995 with regard to IT management. See 44 U.S.C. 3504(a)(1)(B)(vi) (OMB); 44 U.S.C. 3506(h)(5) (agencies).

²¹ We have made recommendations to improve OMB's process for monitoring high-risk IT investments; see GAO, *Information Technology: OMB Can Make More Effective Use of Its Investment Reviews*, [GAO-05-276](#) (Washington, D.C.: Apr. 15, 2005).

²² This policy is set forth and guidance is provided in OMB Circular No. A-11, Part 7, Sec. 300, et seq. (July 2010), and in the Supplement to Part 7, Capital Programming Guide (June 2006), which directs agencies to develop, implement, and use a capital programming process to build their capital asset portfolios.

²³ GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009); [GAO-04-394G](#); [GAO-03-584G](#); and *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making*, [GAO/AIMD-10.1.13](#) (Washington, D.C.: February 1997).

incorporates considerations such as technology opportunities, marketplace trends, fiscal and budgetary constraints, institutional system development and acquisition capabilities, legacy and new system dependencies and life expectancies, and the projected value of competing investments.

The suite of products adopted for a given entity's enterprise architecture, including its structure and content, is largely governed by the framework used to develop the architecture. Since the 1980s, various architecture frameworks have been developed, such as John A. Zachman's "A Framework for Information Systems Architecture,"²⁴ and the DOD Architecture Framework.²⁵

The importance of developing, implementing, and maintaining an enterprise architecture is a basic tenet of both organizational transformation and systems modernization. Managed properly, an enterprise architecture can clarify and help optimize the interdependencies and relationships among an organization's business operations and the underlying IT infrastructure and applications that support these operations. Moreover, when an enterprise architecture is employed in concert with other important management controls, such as portfolio-based capital planning and investment control practices, the architecture can greatly increase the chances that an organization's operational and IT environments will be configured to optimize mission performance. The alternative, as our work has shown, is the perpetuation of the kinds of operational environments that burden many agencies today, where a lack of integration among business operations and the IT

²⁴J. A. Zachman, "A Framework for Information Systems Architecture," *IBM Systems Journal* 26, no. 3 (1987).

²⁵DOD, *Department of Defense Architecture Framework*, version 2.0, Volumes I-III (May 2009).

resources supporting them leads to systems that are duplicative, poorly integrated, and unnecessarily costly to maintain and interface.²⁶

In February 2002 and April 2003, we issued versions 1.0 and 1.1 of our *Enterprise Architecture Management Maturity Framework*; in August 2010, we issued a major revision (version 2.0).²⁷ The framework provides a standard yet flexible benchmark against which to determine where the enterprise stands in its progress toward the ultimate goal: having a continuously improving enterprise architecture program that can serve as a featured decision support tool when considering and planning large-scale organizational restructuring or transformation initiatives. In addition, it also provides a basis for developing architecture management improvement plans, as well as for measuring, reporting, and overseeing progress in implementing these plans.

Several approaches to structuring enterprise architecture exist and can be applied to the extent that they are relevant and appropriate for a given enterprise. In general, these approaches provide for decomposing an enterprise into its logical parts and architecting each of the parts in relation to enterprisewide needs and the inherent relationships and dependencies that exist among the parts. As such, the approaches are fundamentally aligned and consistent with a number of basic enterprise architecture principles, such as incremental rather than monolithic architecture development and implementation, optimization of the whole rather than optimization of the component parts, and maximization of shared data and services across the component parts rather than duplication. Moreover, these approaches are not mutually exclusive and, in fact, can all be applied to some degree for a given enterprise, depending on the characteristics and circumstances of that enterprise. The approaches, which are briefly described here, are federated, segmented, and service-oriented.

²⁶ GAO, *Federal Aviation Administration: Stronger Architecture Program Needed to Guide Systems Modernization Efforts*, [GAO-05-266](#) (Washington, D.C.: Apr. 29, 2005); *Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*, [GAO-04-777](#) (Washington, D.C.: Aug. 6, 2004); [GAO-04-731R](#); *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, [GAO-04-43](#) (Washington, D.C.: Nov. 21, 2003); [GAO-03-1018](#); [GAO-03-877R](#); *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, [GAO-01-631](#) (Washington, D.C.: June 29, 2001); and *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, [GAO/AIMD-00-212](#) (Washington, D.C.: Aug. 1, 2000).

²⁷ [GAO-10-846G](#).

Federated

Under a federated approach, the architecture consists of a family of coherent but distinct member architectures that conform to an overarching corporate or parent architecture. This approach recognizes that each federation member has unique goals and needs as well as common roles and responsibilities with the members above and below it. As such, member architectures (e.g., component, subordinate, or subsidiary architectures) are substantially autonomous, but they also inherit certain rules, policies, procedures, and services from the parent architectures. A federated architecture enables component organization autonomy while ensuring corporate or enterprisewide linkages and alignment where appropriate.

Segmented

A segmented approach to enterprise architecture development and use, like a federated approach, employs a “divide and conquer” methodology in which architecture segments are identified, prioritized, developed, and implemented. In general, segments can be viewed as logical aspects, or “slivers,” of the enterprise that can be architected and pursued as separate initiatives under the overall corporate architecture. As such, the segments serve as a bridge between the corporate frame of reference captured in the enterprise architecture and individual programs within portfolios of system investments. OMB has issued guidance related to segment architectures.²⁸ As part of its guidance, agencies are to group segments into three categories: core mission areas (e.g., air transportation), business services (e.g., financial management), and enterprise services (e.g., records management).

Service-Oriented

A service-oriented approach to enterprise architecture is intended to identify and promote the shared use of common business capabilities across the enterprise. Under this approach, functions and applications are defined and designed as discrete and reusable capabilities or services that may be under the control of different organizational entities. As such, the capabilities or services need to be, among other things, (1) self-contained, meaning that they do not depend on any other functions or applications to execute a discrete unit of work; (2) published and exposed as self-describing business capabilities that can be accessed and used; and (3) subscribed to via well-defined and standardized interfaces. This approach

²⁸OMB, *Improving Agency Performance Using Information and Information Technology* (Enterprise Architecture Assessment Framework v3.1), (Washington, D.C.: June 2009); *Federal Segment Architecture Working Group* and OMB, *Federal Segment Architecture Methodology*, version 1.0 (Washington, D.C.: December 2008); and OMB, *Federal Enterprise Architecture Practice Guidance* (Washington, D.C.: November 2007).

is intended to reduce redundancy and increase integration, as well as provide the flexibility needed to support a quicker response to changing and evolving business requirements and emerging conditions.

IT Investment Management: A Brief Description

IT investment management is a process for linking investment decisions to an organization's strategic objectives and business plans that focuses on selecting, controlling, and evaluating investments in a manner that minimizes risks while maximizing the return of investment.²⁹

- During the selection phase, the organization (1) identifies and analyzes each project's risks and returns before committing significant funds to any project and (2) selects those IT projects that will best support its mission needs.
- During the control phase, the organization ensures that, as projects develop and investment expenditures continue, the projects meet mission needs at the expected levels of cost and risk. If the project is not meeting expectations, or if problems arise, steps are quickly taken to address the deficiencies.
- During the evaluation phase, actual versus expected results are compared once a project has been fully implemented. This is done to (1) assess the project's impact on mission performance, (2) identify any changes or modifications to the project that may be needed, and (3) revise the investment management process based on lessons learned.

Consistent with this guidance, our IT Investment Management (ITIM) framework consists of five progressive stages of maturity for any given agency relative to selecting, controlling, and evaluating its investment management capabilities.³⁰ (See fig. 2 for the five ITIM stages of maturity.) The overriding purpose of the framework is to encourage investment selection and control and to evaluate processes that promote business value and mission performance, reduce risk, and increase accountability

²⁹GAO-04-394G; GAO/AIMD-10.1.13; GAO, *Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology*, GAO/AIMD-94-115 (Washington, D.C.: May 1994); and OMB, *Evaluating Information Technology Investments, A Practical Guide* (Washington, D.C.: November 1995).

³⁰GAO-04-394G.

and transparency. We have used the framework in many of our evaluations, and a number of agencies have adopted it.³¹

In our ITIM framework, with the exception of the first stage, each maturity stage is composed of “critical processes” that must be implemented and institutionalized in order for the organization to achieve that stage. Each ITIM critical process consists of “key practices” (organizational structures, policies, and procedures) that must be executed to implement the critical process. Our research shows that agency efforts to improve investment management capabilities should focus on implementing all lower-stage practices before addressing the higher-stage practices.

³¹GAO, *Information Technology: HUD Needs to Better Define Commitments and Disclose Risks for Modernization Projects in Future Expenditure Plans*, [GAO-11-72](#) (Washington, D.C.: Nov. 23, 2010); *Information Technology: HUD Needs to Strengthen Its Capacity to Manage and Modernize Its Environment*, [GAO-09-675](#) (Washington, D.C.: July 31, 2009); *Information Technology: FDA Needs to Establish Key Plans and Processes for Guiding Systems Modernization Efforts*, [GAO-09-523](#) (Washington D.C.: June 2, 2009); *Information Technology: SSA Has Taken Key Steps for Managing Its Investments, but Needs to Strengthen Oversight and Fully Define Policies and Procedures*, [GAO-08-1020](#) (Washington, D.C.: Sept. 12, 2008); *Information Technology: Treasury Needs to Strengthen Its Investment Board Operations and Oversight*, [GAO-07-865](#) (Washington, D.C.: July 23, 2007); *Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments*, [GAO-07-424](#) (Washington, D.C.: Apr. 27, 2007); *Information Technology: Centers for Medicare & Medicaid Services Needs to Establish Critical Investment Management Capabilities*, [GAO-06-12](#) (Washington, D.C.: Oct. 28, 2005); *Information Technology: HHS Has Several Investment Management Capabilities in Place, but Needs to Address Key Weaknesses*, [GAO-06-11](#) (Washington, D.C.: Oct. 28, 2005).

Figure 2: The Five ITIM Stages of Maturity with Critical Processes

Maturity stages	Critical processes
Stage 5: Leveraging IT for strategic outcomes	<ul style="list-style-type: none">- Optimizing the investment process- Using IT to drive strategic business change
Stage 4: Improving the investment process	<ul style="list-style-type: none">- Improving the portfolio's performance- Managing the succession of information systems
Stage 3: Developing a complete investment portfolio	<ul style="list-style-type: none">- Defining the portfolio criteria- Creating the portfolio- Evaluating the portfolio- Conducting postimplementation reviews
Stage 2: Building the investment foundation	<ul style="list-style-type: none">- Instituting the investment board- Meeting business needs- Selecting an investment- Providing investment oversight- Capturing investment information
Stage 1: Creating investment awareness	IT spending without disciplined investment processes

Source: GAO.

Stage 2 critical processes lay the foundation by establishing successful, predictable, and repeatable investment control processes at the project level. Stage 3 is where the agency moves from project-centric processes to portfolio-based processes and evaluates potential investments according to how well they support the agency's missions, strategies, and goals. Organizations implementing these Stage 2 and 3 practices have in place selection, control, and evaluation processes that are consistent with the Clinger-Cohen Act.³² Stages 4 and 5 require the use of evaluation techniques to continuously improve both investment processes and portfolios in order to better achieve strategic outcomes.

Our research shows that agency efforts to improve investment management capabilities should focus on implementing all lower-stage practices before addressing the higher-stage practices and therefore our reviews tend to focus on Stage 2 and Stage 3 critical processes. Specifically, within Stage 2, there are five critical processes and nine associated key practices (known as organizational commitments) that call for policies and procedures associated with effective project-level management. These are shown in table 1.

³² 40 U.S.C. §§ 11311-11313.

Table 1: Stage 2 Critical Processes and Associated Key Practices

Critical process	Purpose	Associated key practices
Instituting the investment board	To define and establish an appropriate IT investment management structure and the processes for selecting, controlling, and evaluating IT investments	1. An enterprisewide IT investment board composed of senior executives from IT and business units is responsible for defining and implementing the organization's IT investment governance process. 2. The organization has a documented IT investment process directing each investment board's operations.
Meeting business needs	To ensure that IT projects and systems support the organization's business needs and meet users' needs.	3. The organization has documented policies and procedures for identifying IT projects or systems that support the organization's ongoing and future business needs.
Selecting an investment	To ensure that a well-defined and disciplined process is used to select new IT proposals and reselect ongoing investments.	4. The organization has documented policies and procedures for selecting new IT proposals. 5. The organization has documented policies and procedures for reselecting ongoing IT investments. 6. The organization has policies and procedures for integrating funding with the process of selecting an investment.
Providing investment oversight	To review the progress of IT projects and systems, using predefined criteria and checkpoints in meeting cost, schedule, risk, and benefit expectations and to take corrective action when these expectations are not being met.	7. The organization has documented policies and procedures for management oversight of IT projects and systems.
Capturing investment information	To make available to decision makers information to evaluate the impacts and opportunities created by proposed (or continuing) IT investments.	8. The organization has documented policies and procedures for identifying and collecting information about IT projects and systems to support the investment management process. 9. An official is assigned responsibility for ensuring that the information collected during project and systems identification meets the needs of the investment management process.

Source: GAO.

Within Stage 3, there are four critical processes and five associated key practices (known as organizational commitments) that call for policies and procedures associated with effective portfolio-based investment management. These are shown in table 2.

Table 2: Stage 3 Critical Processes and Associated Key Practices

Critical process	Purpose	Associated key practices
Defining the portfolio criteria	To ensure that the organization develops and maintains IT portfolio selection criteria that support its mission, organizational strategies, and business priorities.	<ol style="list-style-type: none"> 1. The organization has documented policies and procedures for creating and modifying IT portfolio selection criteria. 2. Responsibility is assigned to an individual or group for managing the development and modification of the IT portfolio selection criteria.
Creating the portfolio	To ensure that IT investments are analyzed according to the organization's portfolio selection criteria and to ensure that an optimal IT investment portfolio with manageable risks and returns is selected and funded.	<ol style="list-style-type: none"> 3. The organization has documented policies and procedures for analyzing, selecting, and maintaining the investment portfolio.
Evaluating the portfolio	To review the performance of the organization's investment portfolios at agreed-upon intervals and to adjust the allocation of resources among investments as necessary.	<ol style="list-style-type: none"> 4. The organization has documented policies and procedures for reviewing, evaluating, and improving the performance of its portfolios.
Conducting post-implementation reviews	To compare the results of recently-implemented investments with the expectations that were set for them and to develop a set of lessons learned from these reviews.	<ol style="list-style-type: none"> 5. The organization has documented policies and procedures for conducting post-implementation reviews.

Source: GAO.

DOD's Institutional Approach to Business Systems Modernization

The NDAA for Fiscal Year 2008 designated the Deputy Secretary of Defense position as the Chief Management Officer for DOD and created a deputy position to assist the Chief Management Officer.³³ The Chief Management Officer's responsibilities include developing and maintaining a departmentwide strategic plan for business reform and establishing performance goals and measures for improving and evaluating overall economy, efficiency, and effectiveness, and monitoring and measuring the progress of the department. The Deputy Chief Management Officer's responsibilities include recommending to the Chief Management Officer methodologies and measurement criteria to better synchronize, integrate, and coordinate the business operations to ensure alignment in support of the warfighting mission. The Business Transformation Agency supports the Deputy Chief Management Officer in leading and coordinating

³³ Pub. L. No. 110-181, § 904, 122 Stat. 3, 273 (Jan. 28, 2008).

business transformation efforts across the department. This includes maintaining and updating the department's enterprise architecture for its business mission area.³⁴

The Chief Management Officer and Deputy Chief Management Officer are to interact with several entities to guide the direction, oversight, and execution of DOD's business transformation efforts, which include business systems modernization. These entities include the Defense Business Systems Management Committee, which serves as the highest-ranking investment review and decisionmaking body for business systems modernization activities and is chaired by the Deputy Secretary of Defense; the principal staff assistants, who serve as the certification³⁵ authorities for business system modernizations in their respective core business missions; the investment review boards (IRB),³⁶ which are chaired by the certifying authorities and form the review and decision-making bodies for business system investments in their respective areas of responsibility; and the Business Transformation Agency, which is responsible for supporting the IRBs and for leading and coordinating business transformation efforts across the department. In August 2010 and in January 2011, the Secretary of Defense announced the plans to disestablish the Business Transformation Agency and the Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense CIO (ASD(NII)/DOD CIO) (who is a member of the Defense Business Systems Management Committee), respectively. According to DOD officials, the mission of the Office of the Deputy Chief Management Officer duplicates many of the Business

³⁴According to DOD, the business mission area is responsible for ensuring that capabilities, resources, and materiel are reliably delivered to the warfighter. Specifically, the business mission area addresses areas, such as real property and human resources management.

³⁵The act (10 U.S.C. § 2222(a), as amended), requires designated approval authorities to certify that a defense business system modernization (1) has been determined by the appropriate Chief Management Officer to (a) be in compliance with the enterprise architecture and (b) have undertaken appropriate business process re-engineering efforts; (2) is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or (3) is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such an adverse effect.

³⁶These investment review boards are for Financial Management, Weapon Systems Lifecycle Management and Materiel Supply and Services Management, Real Property and Installations Lifecycle Management, and Human Resources Management. In August 2009, DOD's Enterprise Guidance Board was chartered as the DOD CIO's Investment Review Board.

Transformation Agency functions. They added that rather than lead in the development of better business practices, the agency’s prime focus has changed to the management of several relatively small business systems and providing direct support to the Deputy Chief Management Officer on various policy issues. As a result, according to these officials, the narrower function does not justify continuing the Business Transformation Agency as a stand-alone defense agency.

The Secretary of Defense also directed that the remaining functions of the Business Transformation Agency be reviewed and transferred to other organizations in DOD, as appropriate and that the disestablishment of the agency should be no later than June 30, 2011. However, as of June 2011, these implementation decisions had yet to be made and both the Business Transformation Agency and the Office of the ASD (NII)/DOD CIO organizations were still in operation.

Table 3 lists governance entities and provides greater detail on their roles, responsibilities, and composition.

Table 3: DOD Business Systems Modernization Governance Entities’ Roles, Responsibilities, and Composition		
Entity	Roles and responsibilities	Composition
Defense Business Systems Management Committee	<p>Provides strategic direction and plans for the business mission area in coordination with the warfighting and enterprise information environment mission areas.^a</p> <p>Recommends policies and procedures required to integrate DOD business transformation and attain cross-department, end-to-end interoperability of business systems and processes.</p> <p>Serves as approving authority for business system modernizations greater than \$1 million.</p> <p>Establishes policies and approves the business mission area strategic plan, the enterprise transition plan for implementation of business systems modernization, the transformation program baseline, and the business enterprise architecture.</p>	<p>Chaired by the Deputy Secretary of Defense/Chief Management Officer; the Vice Chair is the Deputy Chief Management Officer. Includes senior leadership in the Office of the Secretary of Defense, such as the Assistant Secretary of Defense for Network and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DOD CIO). Also includes the Military Department Chief Management Officers, the heads of select defense agencies, and other senior participation by the Joint Chiefs of Staff and the U.S. Transportation Command.</p>

Entity	Roles and responsibilities	Composition
Principal Staff Assistants/Certification Authorities	<p>Support the Defense Business Systems Management Committee's management of enterprise business IT investments.</p> <p>Serve as the certification authorities accountable for the obligation of funds for respective business system modernizations within designated core business missions.^b</p> <p>Review, approve, and oversee the planning, design, acquisition, deployment, operation, maintenance, and modernization of the defense business systems assigned.</p> <p>Provide the Defense Business Systems Management Committee with recommendations for system investment approval.</p> <p>Provide input into enterprise-level architecture products and transition plans that support their core business mission.</p>	Under Secretaries of Defense for Acquisition, Technology, and Logistics; Comptroller; and Personnel and Readiness; ASD(NII)/DOD CIO; and the Deputy Secretary of Defense.
Investment Review Boards	<p>Serve as the oversight and investment decision making bodies for those business capabilities that support activities under their designated areas of responsibility.</p> <p>Review and recommend certification for all business systems modernization investments costing more than \$1 million that are integrated and compliant with the business enterprise architecture.</p>	Includes the principal staff assistants, Joint Staff, ASD(NII)/DOD CIO, core business mission area representatives, military departments, defense agencies, and combatant commands.
Component Precertification Authority ^c	<p>Ensures component-level investment review processes integrate with the investment management system.</p> <p>Identifies those component systems that require investment review board certification and prepare, review, approve, validate, and transfer investment documentation as required.</p> <p>Assesses and pre-certifies business process re-engineering efforts and architecture compliance of component systems submitted for certification and annual review.</p>	Includes the Chief Management Officer from Air Force, the Army, the Navy, and the DOD Deputy Chief Management Officer representing the defense agencies or a business system supported by more than one military department or defense agency.

Entity	Roles and responsibilities	Composition
Business Transformation Agency	<p>Operates under the authority of the Deputy Chief Management Officer.</p> <p>Maintains and updates the department's business enterprise architecture and enterprise transition plan.</p> <p>Ensures that functional priorities and requirements of various defense components, such as the Army and the Defense Logistics Agency, are reflected in the architecture.</p> <p>Ensures adoption of DOD-wide information and process standards as defined in the architecture.</p> <p>Serves as the day-to-day management entity of the business transformation effort at the DOD enterprise level.</p> <p>Provides support to the investment review boards.</p>	<p>Composed of eight directorates (Chief of Staff, Defense Business Systems Acquisition Executive, Enterprise Integration, Enterprise Planning and Investment, Transformation Priorities and Requirements Financial Management, Transformation Priorities and Requirements Human Resource Management, Transformation Priorities and Requirements Supply Chain Management, and Warfighter Requirements).</p>

Source: GAO based on DOD documentation.

^aAccording to DOD, the business mission area is responsible for ensuring that capabilities, resources, and materiel are reliably delivered to the warfighter. Specifically, the business mission area addresses areas such as real property and human resources management.

^bDOD has five core business missions: Human Resources Management, Weapon Systems Lifecycle Management, Materiel Supply and Service Management, Real Property and Installations Lifecycle Management, and Financial Management.

^cIn the military departments, the Chief Management Officer is the precertification authority. For the defense agencies, precertification activities are performed by the component, and the DOD Deputy Chief Management Officer is the precertification authority. These precertification activities result in a Chief Management Officer Determination Memorandum.

Overview of DOD's Tiered Accountability for Business Systems Modernization

Since 2005, DOD has employed a "tiered accountability" approach to business systems modernization. Under this approach, responsibility and accountability for business architectures and systems investment management are assigned to different levels in the organization. For example, the Business Transformation Agency is responsible for developing the corporate business enterprise architecture (i.e., the thin layer of DOD-wide policies, capabilities, standards, and rules) and the associated enterprise transition plan. Each component is responsible for defining a component-level architecture and transition plan associated with its own tiers of responsibility and for doing so in a manner that is aligned with (i.e., does not violate) the corporate business enterprise architecture. Similarly, program managers are responsible for developing program-level architectures and plans and for ensuring alignment with the

architectures and transition plans above them. This concept is to allow for autonomy while also ensuring linkages and alignment from the program level through the component level to the corporate level. Table 4 describes the four investment tiers and identifies the associated reviewing and approving entities.

Table 4: DOD Investment Tiers

	Tier description	Reviewing/approving entities
Tier 1	Major automated information system ^a or major defense acquisition program ^b	Investment Review Board and Defense Business Systems Management Committee
Tier 2	Exceeding \$10 million in total development/modernization costs, but not designated as a major automated information system or major defense acquisition program	Investment Review Board and Defense Business Systems Management Committee
Tier 3	Exceeding \$1 million and up to \$10 million in total development/modernization costs	Investment Review Board and Defense Business Systems Management Committee
Tier 4	Investment funding required up to \$1 million	Component-level review only (unless the system or line of business it supports is designated as an interest program by the Investment Review Board chair)

Source: GAO based on DOD documentation.

^aA major automated information system is a program or initiative that is so designated by the ASD(NII)/DOD CIO or that is estimated to require program costs in any single year in excess of \$32 million, total program costs in excess of \$126 million, or total life cycle costs in excess of \$378 million in fiscal year 2000 constant dollars.

^bA major defense acquisition program is an acquisition program that is so designated or estimated by the Under Secretary of Defense for Acquisition, Technology, and Logistics to require an eventual total expenditure for research, development, and test and evaluation of more than \$365 million or, for procurement, of more than \$2.190 billion in fiscal year 2000 constant dollars.

Consistent with the tiered accountability approach, the Fiscal Year 2008 NDAA required the secretaries of the military departments to designate the department under secretaries as chief management officers with primary responsibility for business operations.³⁷ Moreover, the Fiscal Year 2009 Duncan Hunter NDAA required the military departments to establish business transformation offices to assist their chief management officers in the development of comprehensive business transformation plans.³⁸ In

³⁷Pub. L. No. 110-181, § 904(b), 122 Stat. 3, 274.

³⁸Pub. L. No. 110-417, § 908, 122 Stat. 4356, 4569 (Oct. 14, 2008).

response, all of the military departments have designated their respective Under Secretaries as the chief management officers.

We reported in January 2011 that DOD and the military departments had made limited progress in developing business transformation plans that are supported by a strategic planning process and would enable them to align goals and planning efforts and to measure progress.³⁹ Specifically, we reported that DOD had not set up internal mechanisms, such as procedures and milestones, by which it can reach consensus with the military departments and others on priorities, synchronize the development of plans with each other and the budget process, and guide efforts to monitor progress and take corrective action. Therefore, while the military departments were in varying stages of developing business transformation plans, it was unclear to what extent the business transformation priorities for the military departments will be aligned with the priorities identified in DOD's Strategic Management Plan or how these business transformation priorities will influence the department's budget requests. Accordingly, we made recommendations to enhance DOD's ability to set strategic direction for its business transformation efforts, and better align and institutionalize its efforts to develop and implement plans and measure progress against established goals. DOD partially agreed with the recommendations.

DOD's Approach to Certifying Business System Investments

DOD has a two-stage process to select investments, which it refers to as certification and is a key step in its IT investment process that DOD has aimed to model after GAO's ITIM framework. The first stage involves selection of systems using the Joint Capabilities Integration and Development System, the Defense Acquisition System, and the Planning, Programming, Budgeting, and Execution management systems. At this level, proposals and alternatives are viewed and prioritized for system selection. The second stage of selection involves (1) certifying and approving Tiers 1 through 3 investments and (2) elevating certain component investments to an enterprisewide status. More recently, DOD developed Business Capability Lifecycle guidance, dated November 2010, intended to streamline business system acquisition, and investment management processes to better guide and constrain departmentwide systems modernizations.

³⁹GAO, *Defense Business Transformation: DOD Needs to Take Additional Actions to Further Define Key Management Roles, Develop Measurable Goals, and Align Planning Efforts*, [GAO-11-181R](#) (Washington, D.C.: Jan. 26, 2011).

For certification, the IRBs rely on documentation submitted by appropriate chief management officers for the military departments and precertification authorities for the defense agencies. This documentation includes but is not limited to, a memorandum asserting that an investment is compliant with the business enterprise architecture; an economic viability analysis, which addresses the investment's cost and benefits or cost effectiveness; a business process reengineering determination, which identifies the investment's business process weaknesses, gaps, and opportunities for process improvement; and a certification dashboard, which includes cost and schedule status information. DOD guidance also gives the boards broad authority in their certification reviews and actions, thus allowing each board to review and consider whatever investment-related information that it deems appropriate. Moreover, Business Transformation Agency and IRB officials told us that a board is not limited in the conditions it can place on a program. After an IRB review, the Defense Business Systems Management Committee will be notified of all certification decisions and may elect to approve or disapprove a certification. If a certification is approved, the committee will sign an approval memo that warrants the ability to obligate the related funding for the investment.

Under DOD's approach, there are four types of certification actions:

- **Certify:** An IRB certifies the modernization as fully meeting criteria defined in the act and IRB investment review guidance, such as compliance with the business enterprise architecture and the extent to which the investment is consistent with component and department IT investment portfolios, which are asserted by the component Chief Management Officer.

Certify with conditions: An IRB certifies the modernization with the understanding that it will address specific investment review board-imposed conditions. For example, the Army's General Fund Enterprise Business System was certified with a condition to develop a plan for complying with the data standards of DOD's Item Unique Identifier Registry.⁴⁰

⁴⁰The Item Unique Identification Registry is a relational database that is intended to store acquisition and logistics information to track, catalog, and inventory items, such as equipment and spare parts, via machine-readable item identifiers.

-
- **Recertify:** An IRB certifies the obligation of additional modernization funds for a previously-certified modernization investment. For example, the Air Force's Defense Enterprise Accounting and Management System was recertified in September 2010 for \$26.7 million to be spent across fiscal years 2010 and 2011. This recertification was in addition to the approximately \$22.7 million previously certified in December 2009. In addition, a program must request IRB recertification if the program plans to redistribute previously approved modernization funds among multiple fiscal years and this redistribution will result in the funding for any given fiscal year exceeding the previously approved amount by 10 percent or more.
 - **Decertify:** An IRB may decertify or reduce the amount of modernization funds available to an investment when (1) a component reduces funding for a modernization by more than 10 percent of the originally certified amount, (2) the period of certification for a modernization is shortened, or (3) the entire amount of funding is not to be obligated as previously certified. For example, the Special Operations Command's Special Operations Resource Business Information System had about \$4.59 million decertified because funding was reduced by more than 10 percent of the originally certified amount. An investment review board may also decertify a modernization after development has been terminated. For example, DOD reported that approximately \$2.77 million in research, development, test and evaluation funding for the Army's Wounded Warrior Accountability System was decertified because it was determined that the system provided a capability that could be better utilized under another system.

Summary of Fiscal Year 2005 NDAA Requirements

Congress included provisions in the Fiscal Year 2005 NDAA that are aimed at ensuring DOD's development of a well-defined business enterprise architecture and associated enterprise transition plan, as well as the establishment and implementation of effective investment management structures and processes.⁴¹ According to the act, DOD is required to

- develop a business enterprise architecture and an enterprise transition plan for implementing the architecture,
- identify each business system proposed for funding in DOD's fiscal year budget submissions,

⁴¹Pub. L. No. 108-375, § 332 (10 U.S.C. § 2222).

-
- delegate the responsibility for business systems to designated approval authorities within the Office of the Secretary of Defense,
 - require each approval authority to establish investment review structures and processes, and
 - effective October 1, 2005, not obligate appropriated funds for a defense business system modernization with a total cost of more than \$1 million unless the approval authority certifies that the business system modernization meets several conditions.⁴²

The Fiscal Year 2005 NDAA also requires that the Secretary of Defense annually submit to the congressional defense committees a report on the department's compliance with the above provisions.

Recent GAO Reviews of DOD's Business Systems Modernization

Between 2005 and 2008, we reported that DOD had taken steps to comply with key requirements of the Fiscal Year 2005 NDAA relative to architecture development, transition plan development, budgetary disclosure, and investment review, and to satisfy relevant systems modernization management guidance; however, each report also concluded that much remained to be accomplished relative to the act's requirements and relevant guidance.⁴³ We also reported that DOD had fully satisfied the requirement concerning designated approval authorities and continued to certify and approve modernizations costing more than \$1 million. We concluded that the department had made progress in defining

⁴²The act (10 U.S.C. § 2222(a), as amended), requires designated approval authorities to certify that a defense business system modernization (1) has been determined by the appropriate Chief Management Officer to (a) be in compliance with the enterprise architecture and (b) have undertaken appropriate business process re-engineering efforts; (2) is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or (3) is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such an adverse effect.

⁴³GAO, *DOD Business Systems Modernization: Progress in Establishing Corporate Management Controls Needs to Be Replicated Within Military Departments*, [GAO-08-705](#) (Washington, D.C.: May 15, 2008); *DOD Business Systems Modernization: Progress Continues to Be Made in Establishing Corporate Management Controls, but Further Steps Are Needed*, [GAO-07-733](#) (Washington, D.C.: May 14, 2007); *Business Systems Modernization: DOD Continues to Improve Institutional Approach, but Further Steps Needed*, [GAO-06-658](#) (Washington, D.C.: May 15, 2006); and *DOD Business Systems Modernization: Important Progress Made in Establishing Foundational Architecture Products and Investment Management Practices, but Much Work Remains*, [GAO-06-219](#) (Washington, D.C.: Nov. 23, 2005).

and beginning to implement institutional management controls (i.e., processes, structures, and tools). We reiterated existing recommendations to address each of the areas.

In May 2008, we reported that progress in establishing corporate management controls needed to be replicated within the military departments.⁴⁴ For example, we reported that the military departments did not yet have mature enterprise architecture programs. We also reported that they had yet to fully establish key investment review structures and had yet to define related policies and procedures for effectively performing both project-level and portfolio-based investment management. Because we had previously made recommendations to DOD aimed at putting in place the management controls needed to fully comply with the act and related federal guidance, we did not make additional recommendations.

In May 2009, we reported that the pace of DOD's efforts in defining and implementing key institutional modernization management controls had slowed compared with progress made in each of the last four years, leaving much to be accomplished to fully implement the act's requirements and related guidance.⁴⁵ For example:

- The corporate business enterprise architecture had yet to be extended (i.e., federated) to the entire family of business mission area architectures, including using an independent verification and validation (IV&V) agent to assess the components' subsidiary architectures and federation efforts.
- The fiscal year 2009 budget submission included some, but omitted other key information about business system investments, in part because of the lack of a reliable, comprehensive inventory of all defense business systems.
- The business system information used to support the development of the transition plan and DOD's budget requests, as well as certification and annual reviews, was of questionable reliability.
- DOD and the military departments had yet to fully define key practices (i.e., policies and procedures) related to effectively performing both

⁴⁴ [GAO-08-705](#).

⁴⁵ [GAO-09-586](#).

project-level (Stage 2) and portfolio-based (Stage 3) investment management as called for in the ITIM. For example, of the nine Stage 2 key practices and five Stage 3 key practices, DOD had defined four and one, respectively, while Air Force had defined three and one, respectively. Subsequent to our reports, Army reported that it had (as of May 2009) efforts planned and under way to develop effective investment management processes, but the efforts did not fully satisfy any key practices at the time.

- Business system investments costing more than \$1 million continue to be certified and approved, but these decisions were not always based on complete information.

Accordingly, we reiterated existing recommendations to address each of these areas and further recommended that DOD, among other things, improve the quality of investment-related information. DOD partially agreed with our recommendations and described actions being planned or under way to address them. DOD is currently in the process of addressing these recommendations.

In May 2010,⁴⁶ we reported that the scope and completeness of key information provided in the report were limited. Specifically, the report omitted information on the number of business system investment certification actions taken during fiscal year 2009 and did not include performance measures, such as measures of progress against program cost, capability, and benefit commitments. Further, we concluded that certification and approval decisions may not be sufficiently justified because investments were certified and approved without conditions even though our prior reports had identified program weaknesses that were unresolved at the time of certification and approval. Accordingly, we recommended that DOD ensure that the scope and content of future annual reports to Congress on compliance with section 332 of the NDAA for fiscal year 2005 be expanded to include cost, capability, and benefits performance measures for each business system modernization investment and actual performance against these measures as well as all certification actions on its business system modernization investments that were taken in the previous year by the department. In addition, we recommended that DOD guidance be revised to include provisions that

⁴⁶GAO, *Business Systems Modernization: Scope and Content of DOD's Congressional Report and Executive Oversight of Investments Need to Improve*, [GAO-10-663](#) (Washington, D.C.; May 24, 2010).

require investment review board certification submissions to disclose program weaknesses raised by us and the status of actions to address our recommendations to correct the weaknesses to ensure that investment review board certification actions are better informed and justified. DOD agreed with our recommendations.

DOD Continues to Strengthen Management of Its Business Systems Modernization, but Long-standing Challenges Remain

DOD continues to take steps to comply with the provisions of the Fiscal Year 2005 NDAA and to satisfy relevant system modernization management guidance. In particular, DOD released its fiscal year 2011 enterprise transition plan in December 2010, followed by an update to its business enterprise architecture (version 8.0) in March 2011, and its annual report to Congress in May 2011 describing steps that have been taken and are planned relative to the act's requirements. Collectively, these steps address several statutory provisions and best practices concerning the business enterprise architecture, transition plan, budgetary disclosure, and investment review of systems costing in excess of \$1 million. However, challenges that we identified in prior years still need to be addressed in order for the department to be in full compliance with guidance and NDAA requirements. Most notably, the department has yet to extend and evolve its business enterprise architecture to the military departments' architectures and to fully define IT investment management policies and procedures at the DOD enterprise and component levels. DOD officials agreed that additional steps are needed. They said that the lack of progress is due in part to the uncertainty and pending decisions surrounding the roles and responsibilities of key organizations and senior leadership positions, such as the Business Transformation Agency and ASD(NII)/DOD CIO. However, until DOD fully implements these long-standing institutional modernization management controls required by the act, addressed in GAO recommendations, and otherwise embodied in relevant guidance, its business systems modernization will likely remain a high-risk program. As a result, it is important that the department act quickly to resolve pending decisions about roles and responsibilities.

Adopting a Federated Approach to Architecture Continues to Be a Challenge with Much Remaining to Be Accomplished at the Component Level

Among other things, the act requires DOD to develop a business enterprise architecture to cover all defense business systems and their related functions and activities. According to the act, the architecture should extend to all defense organizational components. In 2006, the department adopted an incremental and federated approach to developing such an architecture. Under this approach, the department releases new architecture versions every year that include a corporate business enterprise architecture that is to be augmented by a coherent family of component architectures. As we have previously reported, such an approach is consistent with best practices and appropriate given DOD's scope and size.⁴⁷

On March 18, 2011, DOD released its business enterprise architecture version 8.0, which focuses on improving the department's ability to manage business operations from an end-to-end perspective. This version continues to represent the thin layer of corporate architectural policies, capabilities, rules, and standards that apply DOD-wide (i.e., to all DOD federation members). This means that version 8.0 appropriately focuses on addressing a limited set of enterprise-level (DOD-wide) priorities and provides the overarching and common architectural context that the distinct and autonomous member (i.e., component) architectures inherit. Nevertheless, this also means that version 8.0 does not provide the total federated family of DOD parent and subsidiary architectures for the business mission area. Having such an architecture is dependent on each military department (Air Force, Army, and Navy) having the capability to manage its enterprise architecture and develop the necessary content.

To assist DOD in its architecture federation efforts, we have previously made a number of recommendations. Specifically, in May 2007, we recommended that the department include in its annual report, required under the act, the results of its IV&V contractor's assessment of the completeness, consistency, understandability, and usability of the federated family of architectures.⁴⁸ While DOD agreed with the recommendation, none of its annual reports since 2007, including its latest annual report (issued in May 2011), have included this information. According to Business Transformation Agency officials, IV&V activities

⁴⁷GAO, *DOD Business Systems Modernization: Progress in Establishing Corporate Management Controls Needs to Be Replicated Within Military Departments*, [GAO-08-705](#) (Washington, D.C.: May 15, 2008).

⁴⁸[GAO-07-733](#).

have focused on the corporate business enterprise architecture and not on the entire federated family of architectures. Business Transformation Agency officials provided us with a report dated March 25, 2011, which summarizes selected IV&V contractor observations and recommendations relative to version 8.0's ability to provide a foundation for business enterprise architecture federation. Overall, the summary confirms our findings by stating that, while there has been previous work to develop a business enterprise architecture federation plan, the execution of the federation has yet to be completed. According to Business Transformation Agency officials, the current requirement under the IV&V contract is to provide analysis of the business enterprise architecture. There are no plans for reviewing the military departments' enterprise architectures.

The challenges that the department faces in federating its architecture and the importance of disclosing to congressional defense committees the state of its federation efforts are amplified by our prior report on the state of the military departments' enterprise architecture programs. Specifically, we reported in May 2008 that none of the three military departments could demonstrate through verifiable documentation that it had established all of the core foundational commitments and capabilities needed to effectively manage the development, maintenance, and implementation of an architecture,⁴⁹ as outlined in our *Enterprise Architecture Management Maturity Framework* version 1.1.⁵⁰

Since then, each of the military departments has adopted a federated approach to developing its respective architecture program. However, the extent to which each of their architecture programs has improved since 2008 varies. For example, while all three have or are in the process of establishing an executive committee with responsibility and accountability for the department's enterprise architecture, none have fully developed an enterprise architecture methodology or have a well-defined business enterprise architecture and transition plan to guide and constrain business transformation initiatives. Table 5 provides a description of the military departments' progress relative to those elements that we previously reported as not satisfied by one or more of the military departments.

⁴⁹GAO, *DOD Business Systems Modernization: Military Departments Need to Strengthen Management of Enterprise Architecture Programs*, [GAO-08-519](#) (Washington, D.C.: May 12, 2008).

⁵⁰GAO, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, [GAO-03-584G](#) (Washington, D.C.: April 2003).

(These elements were common to both versions 1.1 and 2.0 of our *Enterprise Architecture Maturity Management Framework*.)⁵¹

Table 5: Description of Progress for Enterprise Architecture Core Elements Previously Reported as Not Fully Satisfied by One or More Military Departments

Core element ^a	2011 evaluation		
	Air Force	Army	Navy
Adequate resources exist	We previously reported this element as being fully satisfied. ^b	According to the Army, not all of their enterprise architecture budgetary needs are met. Officials stated that the majority of Army enterprise architecture efforts are funded in an ad hoc or decentralized process.	We previously reported this element as being fully satisfied. ^b
Committee or group representing the enterprise is responsible for directing, overseeing, and approving the enterprise architecture	According to Air Force officials, three committees with representation across the enterprise have been established to direct, oversee, and approve the architecture. The roles and responsibilities for approving the architecture have been documented in a charter. However the Air Force has yet to document the roles and responsibilities for directing and overseeing the architecture in a charter.	Various enterprisewide executive committees exist that address architecture-related issues. For example, officials stated that the LandWarNet/Battle Command group approves individual architectures and will continue to do so until the Army Architecture Governance Committee is established. Officials also stated that a reason for this delay is that the regulation has not yet been approved. They further reported that the regulation is expected to be published in August 2011 and calls for the Army Architecture Governance Committee to be responsible and accountable for directing, overseeing, and approving the enterprise architecture.	An executive-level committee with representation from across the enterprise to direct and oversee the architecture has been established. The roles and responsibilities for directing and overseeing the architecture have been documented in an approved charter. As of May 2011, this committee became the approval authority for the Navy enterprise architecture and plans to approve version 3.0, scheduled for release by the end of July 2011. However, the charter has yet to be updated to reflect the committee's approval responsibility.

⁵¹ [GAO-03-584G](#) and [GAO-10-846G](#).

Core element ^a	2011 evaluation		
	Air Force	Army	Navy
Program office responsible for enterprise architecture development and maintenance exists	We previously reported this element as being fully satisfied. ^b	Army has yet to establish a program office with responsibility for the department's enterprise architecture development and maintenance. According to Army officials, the Office of Business Transformation oversees the development of the business systems architecture. However, they stated that decisions are yet to be made about how to best approach the establishment of an Army-wide program office. According to officials, a regulation, expected to be published in August 2011, will assign the Office of the Chief Architect with the responsibilities of managing enterprise architecture functions.	Navy has yet to explicitly assign a program office with responsibility for the department's enterprise architecture development and maintenance; instead, the department has identified a small team of people who conduct activities that are typically associated with such an office. The department has no plans for establishing an enterprise architecture program office. According to Navy officials, it is difficult to justify the creation of a large enterprise architecture program office in a fiscally constrained environment.
Enterprise architecture being developed using a framework, methodology, and automated tool.	We previously reported that the Air Force enterprise architecture was being developed using a framework and automated tool. However, a documented methodology that includes defined steps, tasks, standards, tools, techniques, and measures that govern how the architecture is to be developed, maintained, and validated has yet to be developed. Officials stated that the development of a methodology was pushed back due to budget constraints. No time frames have been established for developing such a methodology.	We previously reported that the enterprise architecture was being developed using a framework and automated tool. However, a documented methodology that includes defined steps, tasks, standards, tools, techniques, and measures that govern how the architecture is to be developed, maintained, and validated has yet to be developed.	We previously reported that the enterprise architecture was being developed using a framework and automated tool. However, a documented methodology that includes defined steps, tasks, standards, tools, techniques, and measures that govern how the architecture is to be developed, maintained, and validated has yet to be developed. Officials indicated that there are no specific time frames for when a Navy enterprise architecture methodology will be developed. According to Navy officials, this is due to the department's current focus on other resource-intensive commitments, such as applying the current enterprise architecture content.

Core element ^a	2011 evaluation		
	Air Force	Army	Navy
Written and approved policy exists for enterprise architecture development	We previously reported this element as being fully satisfied. ^b	Army has developed a draft policy that according to officials calls for enterprise architecture development, maintenance, and use; identifies key players, such as the Deputy Under Secretary of the Army, the Army CIO, and Deputy Chief of Staff; and describes the roles, responsibilities, and relationships for these key players. However, the policy has yet to be approved. According to Army officials, the draft policy is expected to be approved in August 2011.	Navy has developed and approved a policy for enterprise architecture development.
Progress against enterprise architecture plans is measured and reported	Enterprise architecture status is reported to the Chief Architect on a quarterly basis. However, this progress is not measured and reported relative to an enterprise architecture plan.	Army-wide architecture development progress is not measured and reported. Specifically, the execution and completion of corporate architecture tasks are not fully defined in an enterprise architecture program plan, work breakdown structure, and schedule.	We previously reported this element as being fully satisfied. ^b
Written and approved policy exists for enterprise architecture maintenance	We previously reported this element as being fully satisfied. ^b	Army has developed a draft policy that according to officials calls for enterprise architecture development, maintenance, and use; identifies key players, such as the Deputy Under Secretary of the Army, the Army CIO, and Deputy Chief of Staff; and describes the roles, responsibilities, and relationships for these key players. However, the policy has yet to be approved.	Navy has developed a policy that calls for the department's CIO to oversee the maintenance of the department's enterprise architecture.
Enterprise architecture products and management processes undergo IV&V	Enterprise architecture products and management processes have not undergone IV&V.	Enterprise architecture products and management processes have not undergone IV&V.	While enterprise architecture products have undergone verification and validation assessments, they were not conducted by an independent body. Moreover, enterprise architecture management processes have not been subject to IV&V.

Core element ^a	2011 evaluation		
	Air Force	Army	Navy
Enterprise architecture products describe the current and target environments and a transition plan	The department continues to develop its corporate and subordinate enterprise architectures that describe aspects of its business environment. However, it has not developed a business enterprise architecture that provides a clear and comprehensive picture of its current and target business environments. In addition, while the department has identified and described business transformation initiatives, it has not developed a business transition plan.	The department has made progress in developing the first version of its business systems architecture and transition plan. However, important enterprise architecture products describing its current and target business environments have not been developed. In addition, its transition plan does not include important elements, such as gap analyses at the enterprise level and for each business function.	The department continues to develop its corporate enterprise architecture that describes aspects of its business environment. It also has developed a business transition plan. However, it has not developed a business enterprise architecture that provides a clear and comprehensive picture of its current and target business environments. In addition, the business transition plan is missing key elements, such as gap analyses.
Committee or group representing the enterprise or the investment review board has approved current version of enterprise architecture	The June 2011 charter for the executive committee includes a requirement for approval of the enterprise architecture. The current version of the enterprise architecture was approved by the CIO, as it was completed prior to the ratification of this charter. According to Air Force officials, executive committee approval will begin with the next version of the architecture.	The executive committee has yet to approve a version of an enterprisewide architecture.	In May 2011, the executive committee became the approval authority for the Navy enterprise architecture and plans to approve version 3.0, scheduled for release by the end of July 2011. However, the charter has yet to be updated to reflect the committee's approval responsibility. Instead, all enterprise architectures to date were approved by another board. However, this board did not include representatives from across the entire organization.
Quality of enterprise architecture products is measured and reported	We previously reported this element as being fully satisfied. ^b	Army does not measure or report the quality of enterprisewide architecture products.	The Navy enterprise architecture IV&V working group assesses the quality of enterprise architecture products against a set of criteria. This assessment is submitted to the Navy enterprise architecture approval board for approval and the results are posted to Navy's internal enterprise architecture communication tool.

Core element ^a	2011 evaluation		
	Air Force	Army	Navy
Written and approved organization policy exists for IT investment compliance with enterprise architecture	We previously reported this element as being fully satisfied. ^b	Army has yet to document the requirement for IT investment compliance with enterprise architecture. Officials stated that, in the future, investments will be required to demonstrate alignment to the business systems architecture, but did not indicate future plans for assessing compliance against the Army's enterprisewide architecture, which is yet to be developed.	Navy has developed a policy that requires all investments registered in its inventory to be assessed annually for compliance with the Navy enterprise architecture.
Enterprise architecture is integral component of IT investment management process	We previously reported this element as being fully satisfied. ^b	The Army did not provide evidence that enterprise architecture is an integral component of its IT investment management process.	Enterprise architecture is a component of Navy's IT investment management process, as investments must be assessed for enterprise architecture compliance during the IT investment management review process.
Enterprise architecture products are periodically updated	We previously reported this element as being fully satisfied. ^b	The Army has yet to develop an enterprisewide architecture, to include architecture products representing its current and target environments. In lieu, the department continues to develop segment architecture products, such as the business systems architecture.	We previously reported this element as being fully satisfied. ^b
IT investments comply with enterprise architecture	While the department has documented compliance criteria, it has yet to provide evidence demonstrating that IT investments have undergone enterprise architecture compliance assessments.	As stated, the Army has yet to develop an enterprisewide architecture against which compliance assessments can be conducted. In addition, no evidence was provided that investments are assessed for compliance with any of the segment architectures. According to Army officials, investments will be required to demonstrate compliance with the Army's business systems architecture.	Navy has documented specific enterprise architecture compliance requirements. Further, Navy provided evidence that compliance assessments were being conducted.
Organization head has approved current version of enterprise architecture	The Air Force CIO, delegated as head of enterprise architecture by the Secretary of the Air Force, has approved the latest version of its enterprise architecture.	As stated, the Army has yet to develop an enterprisewide architecture that would be approved by the Secretary of the Army or a delegated official.	The Navy CIO, who was delegated the responsibility for overseeing the development and maintenance of the Navy enterprise architecture by the Secretary of the Navy, has approved the current version of its enterprise architecture.

Core element ^a	2011 evaluation		
	Air Force	Army	Navy
Return on enterprise architecture investment is measured and reported	The Air Force did not provide evidence demonstrating that return on enterprise architecture investment is measured and reported. Officials stated that a lack of industry-recognized metrics has inhibited the department's ability to develop useful metrics for measuring return on enterprise architecture investment.	As stated, the Army has yet to develop an enterprisewide architecture. Therefore, enterprise architecture return on investment is not measured and reported. In addition, there was no evidence provided that enterprise architecture return on investment for each of its segments is measured and reported.	Navy did not provide evidence demonstrating that return on enterprise architecture investment is measured and reported. Officials stated that a lack of best practices for measuring the value of enterprise architecture has inhibited the department's ability to demonstrate return on investment to corporate-level executives.
Compliance with enterprise architecture is measured and reported	The Air Force has documented enterprise architecture compliance criteria. Officials stated that the Air Force architecting division reports the results of its compliance assessments to the investment review board, which is responsible for final approval of the investment, in the form of a score of either "pass" or "fail" Officials also stated that without a score of "pass" on the architecture component, funding for an investment can be withheld. However, the department has yet to provide evidence demonstrating that IT investments have undergone enterprise architecture compliance assessments.	As stated, Army has yet to develop an enterprisewide architecture against which compliance assessments can be conducted. In addition, there was no evidence provided that showed compliance with any of the segment architectures is measured and reported.	Navy has provided evidence showing that compliance assessments with the Navy enterprise architecture are measured against criteria laid out in the IT investment management process. Final approval decisions are made by the Navy CIO or Deputy CIOs and recorded in the system inventory.

Source: GAO analysis of military departments' documentation.

^aThese core elements represent those that have remained unchanged from version 1.1 to version 2.0 in our Enterprise Architecture Maturity Management Framework or those that have been slightly modified. They also represent only those elements that we previously reported as not being satisfied or being only partially satisfied by one or more military departments.

^bWe did not evaluate the current status of elements that we previously reported as having been satisfied by a military department.

As described in the table, the military departments have made progress in managing their respective enterprise architecture programs since we last reported in 2008. However, each has yet to address key elements, including developing the architecture content, in order to advance to a level that can be considered fully mature. According to DOD officials, the lack of progress in addressing key management elements has been due to the uncertainty and pending decisions surrounding the roles and responsibilities of key organizations and senior leadership positions. Air

Force officials attributed the state of its enterprise architecture program in part to the lack of resources. Army officials also stated that a major challenge has been the lack of resources (i.e., people and funding) due to the shift of resources to higher priority initiatives. Navy officials stated that there is not one overarching reason for the state of the Navy enterprise architecture program but rather a number of reasons, such as limited resources. Navy officials agreed that work remains to be done and stated that they will continue to address the missing elements as they move forward. Although all the military departments reported resources to be a challenge, as noted earlier, DOD requested about \$17.3 billion for its business systems environment. Given the department's prioritization of about \$17 billion, the military department architecture programs have not received resources that they deemed sufficient to meet their needs. What this means is that DOD, as a whole, is not as well positioned as it should be to realize the significant benefits that a well-managed federation of architectures could afford its business systems modernization efforts. We have ongoing work looking at the status of each of the military departments' enterprise architecture programs relative to all the applicable elements in our *Enterprise Architecture Management Maturity Framework* version 2.0.⁵²

Military Departments Continue to Develop Architecture Content, but Have yet to Develop Well-Defined Business Enterprise Architectures and Transition Plans

The Fiscal Year 2009 NDAA⁵³ requires that each military department develop a well-defined enterprisewide business architecture and transition plan encompassing end-to-end business processes and that is capable of providing accurate and timely information in support of business decisions of the military department. However, while each of the departments has taken steps to develop architecture content, none has a well-defined business enterprise architecture and associated transition plan to guide and constrain its business transformation initiatives. Individual examples of progress made and challenges still facing each department are discussed next.

Department of the Air Force

The Department of the Air Force is developing a corporate enterprise architecture and 12 subordinate "sub-enterprise" architectures, each of which is to be supported by subordinate domain architectures (i.e., acquisition), as appropriate. According to Air Force officials, work is still

⁵² [GAO-10-846G](#).

⁵³ Pub. L. No. 110-417, § 908(b)(2), 122 Stat. 4356, 4569 (Oct. 14, 2008).

under way to identify the respective domains and determining which domains will support each sub-enterprise. According to these officials, the Air Force business enterprise architecture was until now being developed as a separate initiative but work is under way to integrate it with the Agile Combat Support sub-enterprise architecture.⁵⁴

In 2008, we reported that, as part of its Agile Combat Support sub-enterprise architecture, the department had developed enterprise architecture products that described some, but not all, elements of its current and target environments as well as a transition plan for its business area. Specifically, we reported that the Air Force had not defined the architecture products that described its logistics enterprise architecture for its current environment and its acquisition enterprise architecture and health services enterprise architectures for its target environments. We also reported that, while it had developed a sequencing plan of systems, it had not defined a gap analysis describing how the department would transition from the current to the target environment. Since then, the department has developed architectural artifacts that capture some of the missing business-related elements. For example, the Air Force has identified acquisition transformation goals, health services operational activities, and logistics systems and services, such as the Commodity Management Service.⁵⁵ In addition, the department has identified and described business transformation initiatives (e.g., streamline civilian hiring process to meet DOD's goal of 80 days by 2012). However, not all important business enterprise architecture contents have been described, including current functional capabilities and data objects necessary for current business operations.

Furthermore, although the department has identified some business-related elements, it does not have a well-defined business enterprise architecture and a transition plan to guide and constrain business transformation initiatives. In particular, it has yet to develop architectural products under its Air Force business enterprise architecture that would describe its current and target business environments in terms of business,

⁵⁴The Agile Combat Support Architecture is planned to include all combat services/support activities and generating force activities of the Air Force, as well as the Air Force business enterprise architecture.

⁵⁵The Commodity Management Service provides functions for creating, configuring, and calculating the data required for watch boards for fuel and ammunition data and empowers the Global Combat Support System–Joint Logistics Management application system.

information/data, application/service, technology, performance, and security. According to the Air Force, it is focused instead on capturing and using existing architecture artifacts that describe current and target architectures associated with priority areas for improvement. In addition, although the Air Force has outlined the business improvement priorities, it has yet to develop an enterprise transition plan for the business environment, including descriptions of gaps in terms of functional capabilities, performance shortfalls of business processes, and potential duplications of system functions.

The department also has yet to determine what, if any, of the business architectural artifacts under the Agile Combat Support sub-enterprise is to be leveraged for the development of the Air Force business enterprise architecture. According to Air Force officials, the Air Force business enterprise architecture and the Agile Combat Support sub-enterprise will use one common set of artifacts, and the department has identified the business architectural artifacts from the Agile Combat Support sub-enterprise to be merged with the Air Force business enterprise architecture. However, we have yet to be provided with a listing of these artifacts. In addition, according to these officials, discussion is still under way on how the department plans to federate the sub-enterprise architectures, including the Agile Combat Support, to the corporate enterprise architecture.

According to Air Force officials, in the future, the Air Force business enterprise architecture will focus on end-to-end processes with defined outputs and it will include an alignment of business systems to these end-to-end business processes. Also, according to the Air Force, it plans to use an architecture-based approach to align current Air Force capabilities and systems against specific business processes to identify duplication or gaps in process-based capabilities. According to the department, an implementation plan will be developed by the end of fiscal year 2011.

Without architectural descriptions of current and target business environments and an associated transition plan, as well as a clear picture of how to leverage prior content in development of the Air Force business enterprise architecture, the department is not well positioned to realize the significant benefits that a well-defined enterprisewide business architecture and transition plan can provide, including objective decision making regarding capability enhancements across end-to-end business processes and resources allocation across business system investments.

Department of the Army

The Department of the Army has yet to develop or establish plans for developing a corporate enterprise architecture that identifies and describes rules, policies, procedures, and services to be federated across the Army. Instead, the department's approach consists of developing three separate and distinct segment architectures (i.e., battle command, networks, and generating force), each of which is being developed by separate department organizational units and is supported by individual segment and solution architectures. According to department officials, the department's current approach to developing its business enterprise architecture calls for this content to be developed as part of the generating force enterprise architecture effort.

In 2008, we reported that Army had not defined its current and target business environments and developed a transition plan. To its credit, the department has since made progress in developing its first version of the Army's business enterprise architecture. Specifically, it has defined the scope of this architecture, which comprises traditional business functions such as acquisition, logistics, financial management, human capital management, and installation and environment. The scope of the Army's business enterprise architecture is also extended to include training and sub-segments of the LandWarNet/Battle Command⁵⁶ functions. This provides logical groupings of the key business activities the department performs, and can be used to identify subordinate architectures that support the department's generating force mission area. In addition, the architecture includes the 15 end-to-end business processes listed in the DOD business enterprise architecture and Army plans to use these processes to guide and constrain business process modeling efforts and identify business systems that are to be integrated. This is consistent with DOD's approach of using end-to-end business processes to optimize business processes and the systems that support them. Further, the department has outlined its business transformation initiatives (e.g., civilian hiring reform) to accelerate business process improvement and cost savings.

⁵⁶The LandWarNet/Battle Command Directorate is the primary Army Staff organization chartered to validate, prioritize, and synchronize Army network requirements across the Army. It is responsible for monitoring the activities and outputs of the various Army agencies that support the development and delivery of the network in order to ensure network and battle command requirements meet Army operational objectives and priorities.

However, Army does not have a well-defined business enterprise architecture and a transition plan to guide and constrain business transformation initiatives. In particular, although the first version provides systems mappings to several end-to-end business processes (e.g., Procure-to-Pay),⁵⁷ it has yet to provide evidence of mappings of system functions to all the end-to-end business processes, such as Service Request-to-Resolution.⁵⁸ According to officials, the mapping of system functions to process steps will take place when the department performs detailed business process mapping. Further, the first version does not describe how end-to-end business processes will be implemented, including principles and guidance for implementing technologies that would support planned business systems investments. Without this, there is an increased risk of incompatible implementation and/or not being able to leverage the most benefits from the technologies.

The Army has also made progress in developing aspects of a business transition plan. For example, it identifies business transformation initiatives, such as civilian hiring reform, and describes results or changes to business operations to be achieved by the business transformation initiatives. It also includes diagrams that depict the migration from legacy business systems to commercial off-the-shelf enterprise resource planning solutions. Such diagrams provide a life cycle view of enterprise systems resources, including describing how each system evolves over time. However, the plan still does not include important content such as gap analyses at the enterprise level and for each business function (e.g. acquisition, financial management) and timelines for addressing the gaps. A gap analysis is an assessment of the differences between the current and target architectures. For example, a performance gap analysis identifies performance measures (e.g., effectiveness) of a business process, highlights which performance measures are not being met in the current environment, and describes performance expectations for these measures in the target environment, thereby describing expected performance improvements of the business process. This performance gap analysis should also identify the business process activities or steps that need to be changed to achieve the future performance expectations. As such, these

⁵⁷Procure-to-Pay encompasses all business functions necessary to obtain goods and services.

⁵⁸Service Request-to-Resolution is the process of performing maintenance on materiel/assets requiring repair or rebuild including the manufacture of parts, modifications, testing, and reclamation.

gap analyses are important to help identify changes or adjustments that are necessary at the enterprise level and within each business function to achieve desired business performance results and mission outcomes.

Department of the Navy

The Department of the Navy's enterprise architecture is comprised of corporate architecture products, which include applicable laws, regulations, and policies as well as enterprisewide reference models and architecture content and subordinate architectures, which comprise nine segment architectures, with each addressing a distinct functional area such as logistics and command and control. These subordinate architectures are to be developed by communities of practice groups that have yet to be formally established. According to Navy officials, the current approach calls for the Navy business enterprise architecture content to be incorporated into the corporate enterprise architecture and applicable segment architectures (e.g., corporate management and support, force support, and logistics segment architectures), as appropriate.

In 2008, our analysis showed that Navy had developed enterprise architecture products that describe some, but not all, elements of its current and target environments as well as a transition plan for its business area. Specifically, we found that the Navy had not defined its current core business processes or provided a comprehensive picture of its current business problems that the department needs to address. We also found that it had yet to develop a well-defined target architecture, including the purpose and scope of all the functional areas (e.g., joint logistics and planning). In addition, we also found that, while the department had developed a transition plan as part of its architecture, the plan was not based on a gap analysis between the current and target environments. This is important to lay out a road map for optimizing mission performance and transforming business operations by systematically implementing changes to technologies and processes.

Since 2008, Navy has identified its business segments such as logistics and force support, representing some of its core business processes. In addition, according to Navy officials, it plans to establish communities of practice to oversee the development of segment reference architectures and a road map for developing these architectures. It has also added additional business-related architecture content. For example, the architecture includes the Navy's Common Operational Activity List that specifies some business activities related to identifying and resolving

accounting records discrepancies. Such operational activities provide a basis from which the department identifies the business activities or functions to be reused (and optimized) across the department and those activities or functions that remain unique to each business segment or domain.

Nonetheless, Navy does not have a well-defined enterprisewide business architecture and transition plan to guide and constrain business transformation initiatives. In particular, the department has not developed a business enterprise architecture that provides a clear and comprehensive picture of its current and target business environments. For example, the enterprise architecture does not describe current and target business capabilities, systems that are to be integrated to support DOD end-to-end business processes, and information exchange requirements among business activities. According to Navy officials, rather than capturing the department's current and target business environments, the focus of Navy's enterprise architecture is to develop artifacts that are "actionable" such as enterprise rules for assessing compliance of business systems. While such actionable artifacts provide value, they do not provide a comprehensive and systematic approach for transforming business operations. Further, there is no evidence that the department has documented current problems or defined the scope and purpose for all of the business-related segment reference architectures. Documenting current problems will enable the Navy to identify opportunities (e.g., new applications, new processes, or new management approaches) for improvement and to assess whether transformation efforts address these problems.

Moreover, although Navy has developed an enterprise transition plan, the plan is not well-defined and does not include an enterprise gap analysis that identifies the differences between the current and target business architectures, particularly the critical differences or shortfalls that affect the successful accomplishment of the department's mission. According to officials, gaps and shortfalls in the current department programs can be identified through enterprise architecture compliance assessments, and enterprise architecture waivers are granted with specific expiration dates and conditions that are to be met to address the gaps and shortfalls. Nevertheless, the focus of these compliance assessments is on gaps and shortfalls of individual programs (e.g., limited system availability) and not on gaps and shortfalls from the perspective of end-to-end business processes (e.g., process gaps) that are needed to achieve the target environment. Moreover, a well-defined business enterprise architecture and transition plan is essential for establishing an implementation road

map to address key gaps and shortfalls that can significantly impact business operations across the department and for evolving and developing business systems that optimize their mission value.

Fiscal Year 2012 Budget Submission Did Not Include Key Information on All Business Systems

Among other things, the Fiscal Year 2005 NDAA requires DOD's annual IT budget submission to include key information on each business system for which funding is being requested, such as the system's designated approval authority and the appropriation type and amount of funds associated with modernization (i.e., development) and current services (i.e., operations and maintenance).

The department's fiscal year 2012 budget submission includes a range of information for 1,637⁵⁹ business system investments.⁶⁰ Of these, 272 involve development and modernization. For each of the 272, the information provided includes the system's name, approval authority, and appropriation type. The submission also identifies the amount of the fiscal year 2012 request that is for development and modernization versus operations and maintenance. For systems in excess of \$1 million in modernization funding, the submission also cites its certification status (e.g., approved, approved with conditions, approved decertification close-out,⁶¹ and withdrawn⁶²) and the Defense Business Systems Management Committee approval date, where applicable.

⁵⁹Of the approximately 2,386 unique investments in DOD's Select and Native Programming Data Input System—Information Technology, 749 are categorized as either national security systems (i.e., intelligence systems, cryptologic activities related to national security, military command and control systems, and equipment that is an integral part of a weapon or weapons system or is critical to the direct fulfillment of military or intelligence missions or systems that store, process, or communicate classified information) or are not within the business mission area (e.g., warfighting mission area).

⁶⁰DOD's budget submission includes funding totals for past, current, and future years. Of the 1,637 business system investments included in the fiscal year 2012 budget submission, 1,440 have requested funding for fiscal year 2012. Further, 272 systems have requested funding for development modernization. The remaining systems have requested funding for current services. A given system could have funding for current services as well as development modernization.

⁶¹The certification status "decertification close-out" identifies a modernization effort that is complete and that does not require any additional funds.

⁶²The certification status "withdrawn" identifies a modernization that is no longer requesting funding for a previously acted-on modernization.

However, similar to prior budget submissions, the fiscal year 2012 budget submission still does not reflect all business system investments. To prepare the submission, DOD relied on business system investment information (e.g., funds requested, mission area, and system description) that is entered by the components into DOD's Select and Native Programming Data Input System—Information Technology (SNAP-IT). In accordance with DOD guidance and according to ASD(NII)/DOD CIO officials, the business systems listed in SNAP-IT should match the systems listed in the Defense Information Technology Portfolio Repository (DITPR)—the department's authoritative business systems inventory. However, the DITPR data provided by DOD in March 2011 included 2,258 business systems. Therefore, SNAP-IT does not reflect about 620 business systems that are identified in DITPR.

We previously reported that the information between SNAP-IT and DITPR were not consistent and accordingly made a recommendation for DOD to develop and implement plans for reconciling and validating the completeness and reliability of information in its DITPR and SNAP-IT system data repositories, and to include information on the status of these efforts in the department's fiscal year 2010 report in response to the act.⁶³ DOD agreed with the need to reconcile information between the two repositories and stated that it had begun to take actions to address this. However, according to the Office of the ASD(NII)/DOD CIO, efforts to provide automated SNAP-IT and DITPR integration work were delayed due to increased SNAP-IT requirements in supporting the fiscal year 2012 budget submission and ongoing reorganization efforts within DOD. The department plans to restart the process of integrating the two systems beginning in the third quarter of fiscal year 2011. Until DOD has a reliable, comprehensive inventory of all defense business systems, it will not be able to ensure the completeness and reliability of the department's IT budget submissions. Moreover, the lack of current and accurate information increases the risk of oversight decisions that are not prudent and justified.

⁶³ [GAO-09-586](#).

DOD Has Continued to Establish Investment Management Processes but Has Yet to Fully Define and Implement Key Practices

Since our 2009 report, DOD has continued to establish investment management processes but has not fully defined all key practices. Further, with regard to certifying and overseeing investments—two key DOD IT management processes for selecting, managing, and monitoring investments—the department largely followed these processes for four department investments we reviewed,⁶⁴ but key steps integral to these processes were not performed. Until DOD fully defines these key practices and performs integral key steps, it is unlikely that the department's reported 2,258 business system investments—totaling \$17.4 billion in fiscal year 2011—will be managed in an effective manner that maximizes mission performance while minimizing or eliminating system overlap and duplication.

DOD Has Continued to Establish Effective Investment Management Processes, but Has Yet to Fully Define Many Key Processes and Associated Policies and Procedures

Since we reported in 2009, DOD has continued to make progress in establishing the kind of investment management processes and associated key practices (i.e., policies and procedures) called for in the act and our ITIM framework⁶⁵ as being integral to effective IT investment management. Specifically, since 2009, Air Force, Navy, and Army have implemented additional key practices associated with effectively managing investments as individual business system programs (Stage 2) and as portfolios of programs (Stage 3), while the DOD-level organizations (herein referred to as DOD enterprise) responsible for DOD-level processes have not. With regard to Stage 2 practices, Navy and Army implemented two key practices, and Air Force implemented one such practice. For Stage 3, Navy implemented one key practice. For those key practices that have yet to be fully defined, DOD enterprise and the military departments have in large part partially defined these practices. Nonetheless, even with this progress, DOD enterprise and the military departments have yet to fully define a majority of the Stage 2 and Stage 3 practices.

Table 6 provides a summary (by DOD enterprise and each military department) of the key Stage 2 practices implemented since 2009 along with those practices we reported in 2009 as having been implemented. The table also includes those practices yet to be implemented. As such, table 6

⁶⁴The investments we reviewed included DOD enterprise-level and military department-level systems: specifically, DOD's Defense Travel System, Air Force's Project Management Resource Tool, Army's Logistics Modernization Program, and Navy's Enterprise Resource Planning system. Details on our methodology for selecting these investments are described in appendix I.

⁶⁵GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C.: March 2004).

provides an overall snapshot of where DOD enterprise and the military departments stand with regard to building their investment management foundation, including the ability to manage investments as individual business system programs.

Table 6: Summary of Key Practices for Stage 2 Critical Processes—Building the Investment Foundation

Critical process	Key practice	DOD enterprise	Air Force	Navy	Army
Instituting the investment board	An enterprisewide IT investment board composed of senior executives from IT and business units is responsible for defining and implementing the organization's IT investment governance process.	●	●	●	○
	The organization has a documented IT investment process directing each investment board's operations.	○	○	○	○
Meeting business needs	The organization has documented policies and procedures for identifying IT projects or systems that support the organization's ongoing and future business needs.	●	●	●	○
Selecting an investment	The organization has documented policies and procedures for selecting a new investment.	○	○	○	○
	The organization has documented policies and procedures for reselecting ongoing investments.	○	○	○	○
	The organization has documented policies and procedures for integrating investment funding with investment selection.	○	○	○	○
Providing investment oversight	The organization has documented policies and procedures for management oversight of IT projects and systems.	○	○	○	○
Capturing investment information	The organization has documented policies and procedures for identifying and collecting information about IT projects and systems to support the investment management process.	●	●	●	●
	An official is assigned responsibility for ensuring that the information collected during project and systems identification meets the needs of the investment management process.	●	●	●	●

Source: GAO.

Key:

- - Key practice was implemented in or before May 2009.
- - Key practice was implemented since May 2009.
- - Key practice is not implemented.

As shown in the table, since 2009:

-
- DOD enterprise has not implemented any additional key practices.
 - Air Force has implemented one key practice—documenting policies for meeting business needs. Specifically, in its IT Investment Review Guide, Air Force defines a process for ensuring that IT business system investments support the department’s ongoing and future business needs. This process includes having an IRB—consisting of senior executives from IT and functional business units, including the Office of the Air Force CIO—to regularly review all business systems, including those in operations and maintenance, to assess their alignment with business needs using factors such as how well investments support the Air Force’s mission and their strategic value and risk.
 - Navy has implemented two additional key practices—(1) instituting an enterprisewide IT investment board and (2) documenting policies for meeting business needs. Specifically, in March 2011, Navy established an Information Enterprise Governance Board—consisting of senior executives from IT and functional business units, including the Navy CIO—to serve as a business systems IRB. Among other things, the board is responsible for business system investment governance, including approving and annually reviewing business system investments. In addition, for meeting business needs, Navy’s Investment Review Guide dated October 2009 defines a process for conducting annual reviews of ongoing IT investments to ensure they support ongoing and future business needs. The process calls for the annual review of all business systems, including those in operations and maintenance, to demonstrate that they support ongoing and future business needs by, among other things, complying with applicable strategic business guidance such as DOD’s business enterprise architecture (BEA).
 - Army has implemented two key practices associated with capturing investment information. First, it has established policies and procedures for collecting information about the department’s investments. Specifically, Army’s investment review guide dated March 2010 defines procedures directing Army’s system owners to submit, update, and maintain IT projects and system information in a departmental data repository called the Army Portfolio Management Solution. Second, Army has assigned responsibility for investment information collection and accuracy. Specifically, Army’s investment review guide states that system owners are responsible for the accuracy of their data in the repository.

With regard to Stage 3 key practices, the following table provides a summary (by DOD enterprise and each military department) of the key practices implemented since 2009 and those practices that have yet to be

implemented. Table 7 provides an overall snapshot of where DOD enterprise and the military departments stand in having the capability to build a complete investment portfolio.

Table 7: Summary of Key Practices for Stage 3 Critical Processes—Developing a Complete Investment Portfolio

Critical process	Key practice	DOD enterprise	Air Force	Navy	Army
Defining the portfolio criteria	The organization has documented policies and procedures for creating and modifying IT portfolio selection criteria.	○	○	○	○
	Responsibility is assigned to an individual or group to manage the development and modification of the IT portfolio selection criteria.	●	●	●	○
Creating the portfolio	The organization has documented policies and procedures for analyzing, selecting, and maintaining the investment portfolios.	○	○	○	○
Evaluating the portfolio	The organization has documented policies and procedures for reviewing, evaluating, and improving the performance of its portfolio(s).	○	○	○	○
Conducting post-implementation reviews	The organization has documented policies and procedures for conducting post-implementation reviews.	○	○	○	○

Source: GAO.

Key:

● - Key practice was implemented in or before May 2009.

● - Key practice was implemented since May 2009.

○ - Key practice is not implemented.

As shown in the table, although DOD enterprise, Air Force, and Army have not implemented additional key practices, Navy has implemented one key practice associated with defining portfolio criteria—assigning responsibility to an individual or group to manage the development and modification of IT portfolio selection criteria. Specifically, Navy developed

guidance that assigns Mission Area Leads⁶⁶ and Functional Area Managers⁶⁷ with responsibility for portfolio selection criteria.

With regard to the Stage 2 and Stage 3 key practices that have yet to be fully implemented, it is important to note that DOD and the military departments have partially defined these practices. For example, for selection, DOD established a process that calls for investments involving more than \$1 million in obligations to be certified and approved before funds are to be expended. Specifically, the process calls for investments to be, among other things, compliant with DOD's BEA and be economically justified. However, the process does not fully address all aspects of the selection key practice. For example, the process does not specify how the IRBs are to use the full range of cost, schedule, and benefit data in making selection (i.e., certification) decisions, as called for in our ITIM framework.

In addition, for oversight, DOD has established an oversight process that calls for, among other things, investments to be reviewed annually to assess how each is performing. As part of the process, the IRBs assess program performance relative to cost, schedule, and capability commitments. However, DOD's oversight process does not provide sufficient visibility into the military department's investment management activities, including its reviews of systems in operations and maintenance and smaller investments, commonly referred to as Tier 4 investments.

Nonetheless, DOD enterprise and the military departments have still not fully defined these Stage 2 and 3 key practices. Specifically, with regard to the nine Stage 2 practices, DOD enterprise, Air Force, and Navy, as shown in table 6, have yet to fully define five key practices (or 56 percent of the practices), and Army has yet to do so for seven (or 78 percent) of the practices.

⁶⁶Mission Area Leads are responsible for managing the IT portfolio for their respective mission area (i.e., Business Mission Area, Intelligence Mission Area, Enterprise Information Environment Mission Area), including developing portfolio guidance, outcome measures, and overseeing the mission area IT portfolio of investments.

⁶⁷Functional Area Managers are to develop and manage functional area (i.e., Human Resource Management, Real Property and Installation Lifecycle Management, Financial Management) IT portfolios. These managers are also responsible for, among other things, recommending, reviewing, and overseeing functional area IT investments.

With regard to the five Stage 3 practices, DOD enterprise, Air Force, and Navy, as shown in table 7, have yet to fully define four key practices (or 80 percent of the practices), and Army has yet to do so for any (100 percent) of the practices.

Officials from DOD enterprise and the military departments attributed the incomplete state of their IT investment management processes to the following:

- DOD enterprise officials said the condition of its processes, including the lack of progress since 2009, was due in part to current ongoing DOD efforts to reorganize the business systems governance organizations (e.g., the Business Transformation Agency) that are responsible for implementing IT investment management at the DOD enterprise level. As noted earlier, in August 2010, the Secretary of Defense announced the plans to disestablish the Business Transformation Agency and that the functions of the Business Transformation Agency, such as its IT investment management function, be reviewed and transferred to other organizations in DOD, as appropriate. The DOD officials stated that these implementation plans have yet to be finalized and have resulted in their investment management implementation efforts being delayed. These officials added that they are aware of the absence of documented project-level and portfolio-level management practices; they also said they are currently working on developing policies and procedures to address the missing processes and practices but were not able to provide us with milestones and a plan with defined steps for when the policies and procedures were to be completed.
- Air Force and Navy officials said their investment management implementation efforts were taking longer than originally planned given their workload and other priorities assigned to them since initiating investment management efforts. They also acknowledged that their processes were missing certain documented project-level and portfolio-level management policies and procedures and said they were in the process of developing policies and procedures to address these missing processes and practices. In particular, Air Force officials stated that they planned to have their policies and procedures approved and finalized by October 2011.
- Army officials said the state of their IT investment management process is due to the fact that the department focused on first establishing selected institutional capabilities—such as defining roles and responsibilities and establishing a department-level IRB—rather than attempting to do everything at once. The officials added that once its initial steps are

completed, Army intends to then focus on implementing remaining Stage 2 and three key processes and practices. Specifically, these officials said that they are aware that Army lacks a military department-level IRB and added that until now they have been relying on functional area experts to review investments before they are sent to the DOD IRBs. They also acknowledged that Army is missing certain documented project-level and portfolio-level management policies and procedures. They further stated that the department is currently working on guidance to address these missing items with the goal of having it approved and finalized by August 2011.

As discussed in our ITIM framework and previous reports on DOD's investment management of its business systems,⁶⁸ adequately documenting both policies and associated procedures that govern how an organization manages its IT projects and investment portfolios is important because doing so provides the basis for rigor, discipline, and repeatability in how investments are selected and controlled across the entire organization. Until DOD fully defines missing policies and procedures, it is unlikely that the department's reported 2,258 business systems will be managed in a consistent, repeatable, and effective manner that, among other things, maximizes mission performance while minimizing or eliminating system overlap and duplication. To this point, there is evidence showing that DOD is not managing its systems in this manner. For example, DOD reported that of its 79 major business and other IT investments, roughly a third are encountering cost, schedule, and performance shortfalls requiring immediate and sustained management attention. In addition, we have consistently reported⁶⁹ for some time that DOD's business system environment has been characterized by (1) little standardization, (2) multiple systems performing the same tasks, (3) the same data stored in multiple systems, and (4) manual data entry into multiple systems. Because DOD spends over \$10 billion each year on its business systems and related IT infrastructure, the potential for identifying and avoiding the

⁶⁸GAO, *Business Systems Modernization: DOD Needs to Fully Define Policies and Procedures for Institutionally Managing Investments*, [GAO-07-538](#) (Washington, D.C.: May 11, 2007); *Business Systems Modernization: Air Force Needs to Fully Define Policies and Procedures for Institutionally Managing Investments*, [GAO-08-52](#) (Washington D.C.: Oct. 31, 2007); *Business Systems Modernization: Department of the Navy Needs to Establish Management Structure and Fully Define Policies and Procedures for Institutionally Managing Investments*, [GAO-08-53](#) (Washington, D.C.: Oct. 31, 2007).

⁶⁹GAO, *Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue*, [GAO-11-318SP](#) (Washington, D.C.: Mar. 1, 2011).

DOD Has Largely Followed Its Certification and Oversight Processes for the Investments Under Review, but Validation and Other Key Steps Were Not Performed

costs associated with duplicative functionality across its business system investments is significant.

As discussed, certification and oversight are key DOD processes for selecting, and overseeing IT investments. DOD guidance⁷⁰ calls for investments to be certified and approved before funds are to be expended on modernization activities. More specifically, the guidance states that investments involving more than \$1 million in obligations are to be certified by designated approval authorities and as part of that certification, authority officials are to attest that each investment

- is compliant with DOD's BEA, including all relevant architecture products, such as products that specify the technical standards needed to promote interoperability among related systems or examine overlaps with other business systems;
- is economically justified, based on an economic viability analysis developed using disciplined and rigorous cost estimating practices; and
- has undergone sufficient business process reengineering analysis, including identifying and developing approaches to streamlining and improving involved processes.

As part of each of these three requirements, we have said it is important for designated approval authorities to validate the results of BEA and other assessments to ensure investment decision making is based on accurate and reliable information.⁷¹ More specifically, we previously reported that DOD had not been performing this step and made recommendations that they do so.⁷² DOD agreed with our findings and recommendations, and stated that it planned to assign validation responsibilities and issue guidance that describes the methodology for performing validation activities but were not able to provide a date for when this would be completed.

⁷⁰DOD, *IT Defense Business Systems Investment Review Process Guidance* (January 2009).

⁷¹GAO, *DOD Business Systems Modernization: Key Navy Programs' Compliance with DOD's Federated Business Enterprise Architecture Needs to Be Adequately Demonstrated*, [GAO-08-972](#) (Washington, D.C.: Aug. 7, 2008).

⁷²[GAO-08-972](#).

Once investments have been certified, DOD guidance calls for investments to be effectively overseen. This includes reviewing annually the progress of investments using predefined criteria and checkpoints, in meeting cost, schedule, risk, and benefit expectations.

Consistent with this, DOD guidance calls for IRBs to annually review certified investments and in doing so, to focus on program performance against cost, schedule, and performance baselines, and progress in meeting the certification conditions discussed. Our ITIM research and experience with federal agencies also shows that it is important for oversight and other decisionmaking authorities to validate performance information used to make decisions so that investment decision making is based on accurate and reliable information.⁷³

Certification

DOD largely followed the certification process for each of the four investments we reviewed, but did not perform validation and other key aspects of the process. Specifically:

BEA compliance. DOD enterprise and the military departments took steps to assess BEA compliance of their respective systems. This included following DOD guidance (the appropriate version of DOD's BEA Compliance Guidance) and using an automated tool (called Architecture Compliance and Requirements Traceability)⁷⁴ to determine and report on the extent of each system's architectural compliance. In addition, in each case, once the BEA assessment had been completed, the appropriate DOD enterprise and military department precertification authorities asserted (via memorandum of certification) that each system was compliant with DOD's BEA.

For example, on the Project Management Resource Tool (PMRT) project, Air Force followed the BEA compliance guidance and used the Architecture Compliance and Requirements Traceability tool to develop a compliance report that mapped BEA activities to PMRT's capabilities. In August 2010, Air Force's Director of Business Transformation and Deputy Chief Management Officer stated in a supporting precertification

⁷³GAO-08-972.

⁷⁴This tool is used to filter BEA segments in an organized manner to facilitate system compliance.

memorandum that this information was used to assert that PMRT was compliant with DOD's BEA.

In another example, on the Defense Travel System, DOD also assessed BEA compliance by using the BEA Compliance Guidance and the Architecture Compliance and Requirements Traceability tool to develop a report showing extent of compliance. In an October 2010, precertification memo, DOD's CIO said this information was used to assert that the system was compliant with DOD's BEA.

Although DOD took these steps to certify BEA compliance, it did not take other key steps. For example, DOD and component designated approval authorities did not validate the assessments and assertions. Specifically, the BEA compliance assessments performed on the investments under review were not validated by DOD certification and approval entities.⁷⁵ Although this was not done, the systems were nevertheless certified as compliant. We reported⁷⁶ on this weakness in 2008 and made recommendations to DOD to, among other things, explicitly assign responsibility for validating program BEA compliance assessments and issue guidance that describes the methodology for performing such validation activities. To date, DOD has yet to implement these recommendations. However, DOD officials told us the department has actions planned or underway to address these recommendations, although they were not able to provide milestones for when this would be accomplished.

In addition, our 2008 report showed that DOD BEA assessments did not include all relevant architecture products, such as products that specify the technical standards needed to promote interoperability among related systems or examine overlaps with other business systems.⁷⁷ Despite the limited assessments, DOD nonetheless certified the investments as BEA compliant even though they did not adequately demonstrate such compliance. Accordingly, we have made recommendations to DOD to revise its BEA compliance guidance, among other things, to address these shortfalls. To date, DOD has yet to implement the recommendations. However, DOD officials said the department has actions planned or

⁷⁵ [GAO-08-972](#).

⁷⁶ [GAO-08-972](#).

⁷⁷ [GAO-08-972](#).

underway to address the recommendations but they were not able to provide a date for when this would be completed.

Economic viability analysis. For the investments under review, DOD enterprise and the military departments used DOD's IT Investment Review Process Guidance (dated January 2009) that specifies how investment economic viability is to be analyzed and assessed. They also used a related automated tool designed to support the development of such analyses. Once the analyses had been performed, the precertification authorities for each of the systems asserted that the efforts had been reviewed, and showed the investments were economically justified to proceed with obligating funds.

For example, on the Logistics Modernization Program, Army used DOD's guidance to conduct its economic viability analysis. The Army also used the economic viability tool to complete the analysis. In addition, in December 2010 memorandum, the Army's Chief Management Officer asserted that the economic viability analysis had been completed, and showed the investment was justified to proceed with obligating funds.

In another example, on the Navy Enterprise Resource Planning system, Navy used the January 2009 DOD guidance to comply with the economic viability analysis requirement and used the economic viability tool to complete the analysis. Further, in a July 2010 memo, the Navy's Chief Management Officer asserted that the investment's economic viability analysis had been completed, and showed the investment was justified to obligate funds.

Although DOD enterprise and the military departments took these steps to justify the investments, they did not perform other key steps. Specifically, DOD enterprise and the military departments did not use important cost estimating practices critical to developing such analyses. For example, in developing its economic justification for its ERP system, Navy did not implement key aspects of earned value management or develop risk mitigation strategies to address this risk. We have previously reported⁷⁸ on these weaknesses and made recommendations to address them. Although the recommendations are still open, DOD enterprise and military

⁷⁸GAO, *DOD Business Systems Modernization: Important Management Controls Being Implemented on Major Navy Program, but Improvements Needed in Key Areas*, [GAO-08-896](#) (Washington, D.C.: Sept. 8, 2008).

department officials have said they have actions planned and under way to address the recommendations. However, they were not able to provide a timetable for when the actions are to be completed.

Business process reengineering assessment. For the investments under review, DOD enterprise and the military departments used DOD's Business Process Reengineering Guidance (dated April 2011) to assess whether the investments complied with the business process reengineering requirement. Consistent with the guidance, DOD enterprise and the military departments completed questionnaires (contained in the guidance) that aim to help DOD enterprise and the military departments identify and develop approaches to streamlining and improving existing business processes. Once these assessments had been completed, the DOD enterprise and military department precertification authorities asserted that business process reengineering assessments had been performed.

For example, on the PMRT project, Air Force used the DOD reengineering guidance to assess whether there were ways to streamline and improve existing business processes to be supported by the system investment. Air Force completed the assessment in July 2010. Air Force reported that as part of this assessment, it had representatives from the offices of the CIO and the Deputy Chief Management Officer review the completed assessment questionnaire and supporting documentation to determine whether the project team had followed the reengineering requirement. Subsequently, in August 2010, the Air Force's Director of Business Transformation and the Deputy Chief Management Officer used this information to assert that sufficient business process reengineering had been conducted in order for the program to obligate investment funding.

While DOD enterprise and military department precertification authorities largely followed DOD's guidance, they did not perform the key step of validating the results of these reengineering assessments to ensure they, among other things, accurately assessed process weaknesses and identified opportunities to streamline and improve affected processes. We have ongoing work on actions the Air Force and Army have taken to comply with statutory requirements regarding business process reengineering.

The reason DOD did not follow key aspects of the certification process—primarily not validating assessment results—is attributed in part to unclear roles and responsibilities. According to military department officials responsible for the investments we reviewed, validation activities

did not occur because DOD policy and guidance does not explicitly require them to be performed and there is no guidance that specifies how assessments should be validated. According to DOD officials, the oversight and designated approval authorities did not validate the DOD enterprise-level assessments and assertions because DOD policy and guidance has not yet been revised to require these authorities to do so. Consequently, until the policy and guidance is updated and roles and responsibilities with regard to who is to perform validation functions are clearly defined, there is an increased risk that DOD will be making business system investment decisions based on information that is inaccurate and unreliable.

Oversight

For the investments under review, DOD largely followed its oversight process but did not perform an important validation activity. Specifically, DOD's oversight process (as specified in the January 2009 Investment Review Guide) calls for investments to be reviewed annually to assess how each is performing. As part of this process, the IRBs assess program performance relative to, among other things, cost, schedule, and capability commitments. The IRBs do this using updated information provided by the programs and screened by DOD enterprise and military department precertification authorities for completeness. These oversight reviews are important because an investment board should have visibility into each project's performance and progress toward predefined cost, schedule, and benefit expectations as well as each project's exposure to risk. Without such visibility and validated information, organizations risk making investment decisions that are inconsistent and are not fully grounded in reliable and accurate data.

Consistent with this direction, DOD conducted (or is planning to conduct) annual reviews for the investments we reviewed.⁷⁹ For example, DOD conducted annual reviews for the Defense Travel System in December 2010 and the Navy Enterprise Resource Planning system in July 2010. In doing these reviews, DOD assessed investment performance using the cost, schedule, and performance information provided by the programs and screened by precertification authorities.

⁷⁹ Air Force officials reported that DOD plans to perform an annual review on PMRT in September 2011.

Although DOD largely followed its oversight process, it did not validate the cost, schedule, and performance information used for decision making. This finding is consistent with our previous report⁸⁰ noting that DOD's oversight process does not provide for sufficient visibility into the military department's investment management activities, including its reviews of systems in operations and maintenance and smaller investments, commonly referred to as Tier 4 investments. Such visibility is important because DOD reports that only 100 of approximately 2,258 total business systems are annually reviewed by the IRBs. This means that the vast majority of business systems are overseen only within the military departments. Accordingly, we have made recommendations to address this area. DOD officials said they plan to address the recommendations but were unable to provide a schedule for when this work is to be completed.

In explaining why the information used by the IRBs is not validated, DOD officials cited the same reasons—outdated policy and guidance and unclear roles and responsibilities—as those provided for the lack of validation in the investment certification process. Consequently, until such roles and responsibilities are clarified, DOD faces increased risk that it will not effectively be able to oversee its extensive business systems investments.

DOD's Annual Report Describes Certification Actions for Its Business System Investments

Among other things, the act⁸¹ requires DOD to submit an annual report to congressional committees on DOD's compliance with requirements of the act, including a description of specific actions the department has taken on each business system modernization investment submitted for certification. The act further requires that such investments involving more than \$1 million in obligations must be certified by a designated approval authority⁸² as meeting specific criteria, such as demonstrating

⁸⁰GAO, *Business Systems Modernization: DOD Needs to Fully Define Policies and Procedures for Institutionally Managing Investments*, [GAO-07-538](#) (Washington, D.C.: May 11, 2007).

⁸¹Section 332 of the Fiscal Year 2005 NDAA (10 U.S.C. § 2222(a), as amended).

⁸²The approval authorities, as discussed earlier in this report, include the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense (Comptroller); the Under Secretary of Defense for Personnel and Readiness; the ASD(NII)/DOD CIO; and the Deputy Secretary of Defense. They are responsible for the review, approval, and oversight of business systems and must establish investment review processes for systems under their cognizance.

compliance with DOD's business enterprise architecture.⁸³ Further, the act requires the Defense Business Systems Management Committee to approve each of these certifications.

In May 2010,⁸⁴ we reported that the department's annual report did not discuss certification actions for all systems on which certification actions had been taken, primarily excluding business system recertifications. We recommended the Deputy Secretary of Defense expand future DOD annual reports to Congress to include all certification actions that had been taken in the previous year by the department on its business system modernization investments. DOD agreed with our recommendation and stated that it would include recertifications in future reports. Since then, the department has addressed this recommendation by including all types of certification actions in its 2011 annual report, including recertification actions. As it has since 2005, DOD continues to certify and approve business system modernization investments in excess of \$1 million.

DOD's annual report identifies IRB certification actions associated with 137 business system investments that underwent the IRB certification and Defense Business Systems Management Committee approval process for fiscal year 2010 and cost approximately \$1.3 billion. Specifically, the annual report accurately states that during fiscal year 2010, 52 unique business system modernizations were certified—35 with and 17 without conditions. For the 35 systems, 32 conditions were reported. Examples of conditions cited in the report are the need for business enterprise architecture compliance to improve interoperability and integration of cross-functional processes and improved program management functions. The report also identifies 93 recertifications and 28 decertifications. For example, the Navy's Enterprise Resource Planning system had about \$7.6 million recertified in early August and another \$96.6 million recertified later in the month.

⁸³The act (10 U.S.C. § 2222(a), as amended), requires designated approval authorities to certify that a defense business system modernization (1) has been determined by the appropriate Chief Management Officer to (a) be in compliance with the enterprise architecture and (b) have undertaken appropriate business process re-engineering efforts; (2) is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or (3) is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such an adverse effect.

⁸⁴[GAO-10-663](#).

While DOD has made progress by reporting its certification actions, the basis for these certification actions and subsequent approvals is limited as discussed in the previous section.

Conclusions

A well-defined federated architecture and accompanying transition plans for the business mission area, along with well-defined investment management policies and procedures across all levels of the department, are critical to effectively addressing DOD's business systems modernization high-risk area. Relatedly, it is important for the department to obtain independent assessments of the completeness, consistency, understandability, and usability of the federated family of business mission area architectures, including associated transition plans. Equally important is for the department to actually implement its architecture and investment management controls in the years ahead on each and every business system investment, and in doing so ensure that it has reliable information on each investment on which to base executive decision making.

DOD has continued to take steps in defining and implementing these key institutional modernization management controls, but challenges that we identified in prior years still need to be addressed. Specifically, while DOD continues to release updates to its corporate enterprise architecture, the architecture has yet to be federated through development of aligned subordinate architectures for each of the military departments. In this regard, each of the military departments has made progress in managing its respective architecture program, but there are still limitations in the scope and completeness, as well as the immaturity of the military department architecture programs, including the completeness of their own transition plans. In addition, while DOD continues to establish investment management processes, the DOD enterprise and the military departments' approaches to business systems investment management still lacks the defined policies and procedures to be considered effective investment selection, control, and evaluation mechanisms. Finally, information used to support the development of DOD's budget requests, as well as to inform certification decisions, is still of questionable reliability. Collectively, these long-standing limitations in the department's institutional modernization management controls continue to put the billions of dollars spent annually on thousands of business system investments at risk. Our previous recommendations to the department have been aimed at accomplishing these and other important activities related to its business systems modernization. To the department's credit,

it has agreed with these recommendations and is committed to implementing them.

However, the state of progress of DOD and military department business system modernization efforts is due, in part, to uncertainty and pending decisions surrounding the roles and responsibilities of key organizations and senior leadership positions. Accordingly, it is essential that DOD resolve these matters expeditiously, as doing so is on the department's critical path for fully establishing the full range of institutional management controls needed to address its business systems modernization high-risk area.

Recommendation for Executive Action

Because we have existing recommendations that address the institutional management control weaknesses discussed in this report, we are making no further recommendations in these areas.

To address the uncertainty and pending decisions surrounding the roles and responsibilities of key organizations, we recommend that the Secretary of Defense expeditiously complete the implementation of the announced transfer of functions of the Business Transformation Agency and the Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense CIO and provide specificity as to when and where these functions will be transferred.

Agency Comments and Our Evaluation

In written comments on a draft of this report, signed by the Deputy Chief Management Officer and reprinted in appendix II, the department agreed with our recommendation and stated that it expects to announce the implementation details concerning the transfer of functions of the Business Transformation Agency and the Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense CIO prior to June 30, 2011.

We support the department's efforts to address our recommendation and reiterate the importance of following through in implementing the recommendation within the stated time frame.

We are sending copies of this report to interested congressional committees; the Director, Office of Management and Budget; and the Secretary of Defense. This report will also be available at no charge on our Web site at <http://www.gao.gov>.

If you or your staffs have any questions on matters discussed in this report, please contact me at (202) 512-6304 or melvinv@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.



Valerie C. Melvin
Director
Information Management and Human Capital Issues

List of Committees

The Honorable Carl Levin
Chairman
The Honorable John McCain
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Daniel Inouye
Chairman
The Honorable Thad Cochran
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Howard P. McKeon
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable C.W. Bill Young
Chairman
The Honorable Norman Dicks
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objective, Scope, and Methodology

As agreed with congressional defense committees, our objective was to assess the actions by the Department of Defense (DOD) to comply with provisions of section 332 of the *Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005*.¹ This included (1) developing a business enterprise architecture and a transition plan for implementing the architecture, (2) identifying systems information in its annual budget submission, (3) establishing a system investment approval and accountability structure along with an investment review process, and (4) certifying and approving any system modernizations costing in excess of \$1 million. (See the background section of this report for additional information on the act's requirements.) Our methodology relative to each of these four provisions is as follows:

- To address the architecture and transition plan provision, we focused on the progress the departments of the Air Force, Army, and Navy have made in developing their respective parts of the federated DOD business enterprise architecture. In doing so, we compared the baseline enterprise architecture program status information as presented in our 2008 report,² with information on the current status of each military department's enterprise architecture program. In doing so, we focused on those select elements that were either similar or slightly modified across versions 1.1 and 2.0 of our *Enterprise Architecture Management Maturity Framework*³ and that were either partially or not satisfied by one or more of the military departments. Specifically, we reviewed written responses and supporting documentation on steps completed, under way, or planned from each military department to identify examples of progress made in addressing those elements that we had previously identified as being not satisfied or partially satisfied. We also reviewed business architectural artifacts to determine the progress each department had made in developing their respective business architectural content since we last reported in 2008.⁴ We interviewed cognizant DOD officials to validate the

¹*Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005*, Pub. L. No. 108-375, § 332, 118 Stat. 1811, 1851-1856 (Oct. 28, 2004), as amended (codified in part at 10 U.S.C. § 2222).

²GAO, *DOD Business Systems Modernization: Military Departments Need to Strengthen Management of Enterprise Architectures*, [GAO-08-519](#) (Washington, D.C.: May 12, 2008).

³GAO, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, [GAO-03-584G](#) (Washington, D.C.: April 2003); and *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)*, [GAO-10-846G](#) (Washington, D.C.: August 2010).

⁴[GAO-08-519](#).

responses and identify any discrepancies. Further, we reviewed the independent verification and validation contractor's statement of work and other work products to determine whether they addressed the department's federated family of corporate and subordinate architectures.

- To determine whether DOD's fiscal year 2012 IT budget submission was prepared in accordance with the criteria set forth in the act, we reviewed and analyzed the *Report on Defense Business System Modernization FY 2005 National Defense Authorization Act, Section 332*, dated March 2011 and compared it to the specific requirements in the act. We also compared information contained in the department's system that is used to prepare its budget submission (SNAP-IT) with information in DOD's Defense Information Technology Portfolio Repository (DITPR) system to determine if DOD's fiscal year 2012 budget request included all business systems. We interviewed Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer officials to discuss the accuracy and comprehensiveness of information contained in the SNAP-IT system, the discrepancies in the information contained in the DITPR and SNAP-IT systems, and efforts under way or planned to address these discrepancies. We did not independently validate the reliability of the cost and budget figures provided by DOD because the specific amounts were not relevant to our findings.
- To assess the establishment of DOD enterprise and component investment management structures and processes, we analyzed whether DOD and its military departments' information technology investment management processes were compliant with federal guidance and the extent to which DOD and the military departments were following their investment management processes, including those at the DOD enterprise-level for approving and certifying investments. To perform the first task, we compared the status of DOD enterprise and military department (Air Force, Army, and Navy) investment management processes—as noted in our May 2009 report⁵ and other sources—with the current status of these organization's processes. As part of this analysis, we focused on the definition of project-level (Stage 2) and portfolio-level (Stage 3) policies and procedures contained in our Information Technology Investment Management (ITIM) Framework⁶ that were identified in our previous work

⁵GAO, *DOD Business Systems Modernization: Recent Slowdown in Institutionalizing Key Management Controls Needs to Be Addressed*, [GAO-09-586](#) (Washington, D.C.: May 18, 2009).

⁶GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C.: March 2004).

as not being established. Specifically, we analyzed written department responses and supporting documentation on steps completed, under way, or planned against ITIM key practices to identify where progress had been made in addressing such previously identified practices. Where there were variances (i.e., support did not show the department was meeting a key practice), we reviewed relevant documentation and interviewed appropriate DOD enterprise and military department officials to identify the causes and impacts.

With regard to our second task, we selected four DOD enterprise-level and military department-level investments that met the following criteria: the investment was (1) either a (Tier 1 or 2) major automated information system from key DOD functional areas (i.e., Weapon Systems Lifecycle Management; Materiel Supply and Services Management; and Human Resources Management) and (2) was at a life cycle phase—such as production and deployment and operations and maintenance—where there were extensive opportunities for system investment officials to demonstrate the organization was following ITIM key practices.⁷ In reviewing these investments, we focused on DOD enterprise and military department activities related to certification and oversight, which are a key part of selecting, managing, and overseeing IT investments as called for in our ITIM framework and DOD guidance. For certification, we reviewed DOD Investment Review Board guidance to understand the types of actions related to the certification of business system modernizations and, in doing so, focused on three certification requirements (e.g., ensuring that designated approval authorities assert that each investment is compliant with the business enterprise architecture). For each requirement, we reviewed supporting documentation from DOD enterprise and the military departments to determine whether there was a documented process for how the requirement was to be certified and to ascertain whether artifacts prepared as part of the process demonstrated that the certification process was being followed. We did the same for the oversight process. When there were variances between the criteria and what DOD enterprise and the military departments had done, we interviewed cognizant DOD enterprise-level and military department-level officials on the causes and impacts.

⁷The DOD-level investment selected was the Defense Travel System. The military-level investments were: Project Management Resource Tool (Air Force), Logistics Modernization Program (Army), and Navy Enterprise Resource Planning system (Navy).

- To determine whether the department was certifying and approving business system investments with annual obligations exceeding \$1 million, we reviewed and analyzed all Defense Business Systems Management Committee certification approval memoranda as well as IRB certification memoranda issued prior to the Defense Business Systems Management Committee's final approval decisions for fiscal year 2010 and compared the results to those certification actions described in the annual report to identify differences. We also reviewed DOD IRB guidance to understand the types of actions related to certification of business system modernizations. We interviewed officials from the Business Transformation Agency and IRBs to discuss any discrepancies.

We conducted this performance audit at DOD and military department offices in Arlington, Virginia, from January 2011 to June 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Department of Defense



DEPUTY CHIEF MANAGEMENT OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, DC 20301-9010

JUN 17 2011

Ms. Valerie Melvin
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Melvin:

This is the Department of Defense response to the U.S. Government Accountability Office (GAO) Draft Report, GAO-11-684, 'DEPARTMENT OF DEFENSE: Further Actions Needed to Institutionalize Key Business System Modernization Management Controls,' dated June 10, 2011 (GAO Code 310961). The Department concurs with the recommendation contained in the draft report.

The Department appreciates the opportunity to respond to your draft report. Should you have any questions, please contact Mr. Bryan Kitchens, Bryan.Kitchens@bta.mil, 703-602-4743.

Sincerely,

A handwritten signature in black ink, appearing to read "E. McGrath", is positioned above the printed name.

Elizabeth A. McGrath

Attachment:
As stated



**GAO DRAFT REPORT DATED JUNE 10, 2011
GAO-11-684 (GAO CODE 310961)**

**“DEPARTMENT OF DEFENSE: FURTHER ACTIONS NEEDED TO
INSTITUTIONALIZE KEY BUSINESS SYSTEM MODERNIZATION
MANAGEMENT CONTROLS”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION**

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense expeditiously complete the implementation of the announced transfer of functions of the Business Transformation Agency (BTA) and the Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/Department of Defense CIO and provide specificity as to when and where these function will be transferred.

DoD RESPONSE: Concur. Announcement of implementation details concerning BTA and NII function transfers is expected to occur prior to June 30, 2011.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Valerie C. Melvin (202) 512-6304 or melvinv@gao.gov

Staff Acknowledgments

In addition to the contact named above, key contributors to this report were Gerard Aflague, Mathew Bader, Carl Barden, Shaun Byrnes, Debra Conner, Elena Epps, Rebecca Eyler, Nancy Glover, Neelaxi Lakhmani (Assistant Director), Anh Le, Lori Martinez, Gary Mountjoy, Freda Paintsil, David Powner (Director), Christine San, Sylvia Shanks, Donald Sebers, Teresa Smith, Jennifer Stavros-Turner, and Adam Vodraska.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

